NETGEAR®

N300 Wireless ADSL2+ Modem Router DGN2200v3

User Manual

October 2013
202-10870-04

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx.*

Trademarks

Contents

Chapter 4 NETGEAR genie Advanced Home

Chapter 5 USB Storage

Chapter 6 Security

Chapter 7   Administration

Chapter 8   Advanced Settings

Chapter 9   Virtual Private Networking

Hardware Setup

1

Getting to know your modem router

The N300 Wireless ADSL2+ Modem Router DGN2200v3 provides you with an easy and secure way to set up a wireless home network with fast access to the Internet over a high-speed digital subscriber line (DSL). It has a built-in DSL modem, is compatible with all major DSL Internet service providers, lets you block unsafe Internet content and applications, and protects the devices (computers, gaming consoles, and so on) that you connect to your home network.

If you have not already set up your new modem router using the installation guide that comes in the box, this chapter walks you through the hardware setup. *Chapter 2, Getting Started with NETGEAR genie*, explains how to set up your Internet connection.

This chapter contains the following sections:

- *Unpack Your Modem Router*
- *Hardware Features*
- *Position Your Modem Router*
- *ADSL Microfilters*
- *Cable Your Modem Router*
- *Verify the Cabling*

For more information about the topics covered in this manual, visit the support website at *http://support.netgear.com*.

If you want instructions about how to wall-mount your router, see Wall-Mount Your Router at *http://support.netgear.com/app/answers/detail/a_id/18725*.

Unpack Your Modem Router

Your box should contain the following items:

- N300 Wireless ADSL2+ Modem Router DGN2200v3
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable with RJ-11 connector
- Microfilters and splitters (quantity and type vary by region)
- CD with documentation (German only)
- Installation guide with cabling and modem router setup instructions

Hardware Features

Before you cable your modem router, take a moment to become familiar with the label and the front and back panels. Pay particular attention to the LEDs on the front panel.

Label

The label on the bottom of the modem router shows the Restore Factory Settings button, , preset login information, MAC address, and serial number.
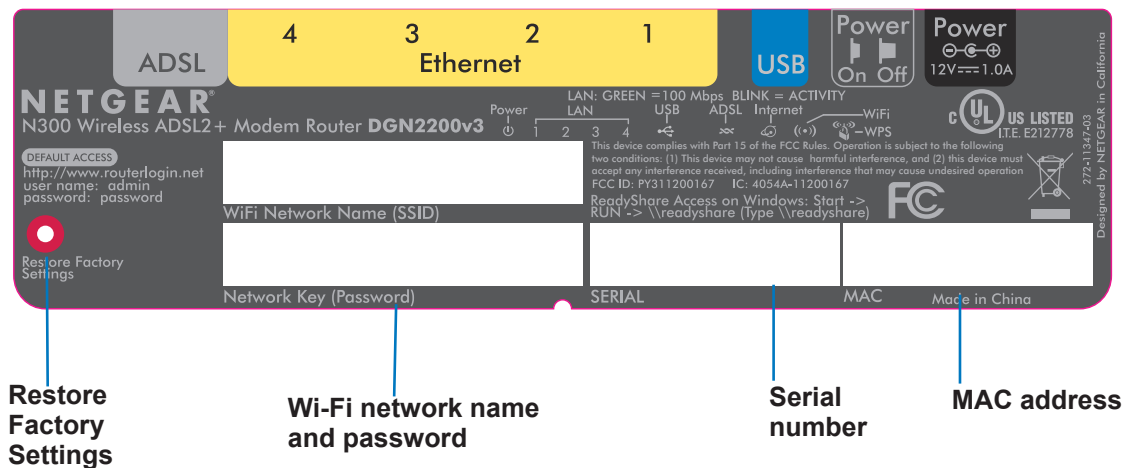
Figure 1. Label on modem router bottom

See *Factory Settings* on page 134 for information about restoring factory settings.

Back Panel

The back panel has the On/Off button and port connections as shown in the figure.

ADSL　　　　　　　　**USB**　　**Power**

Ethernet LAN　　　**On/Off**
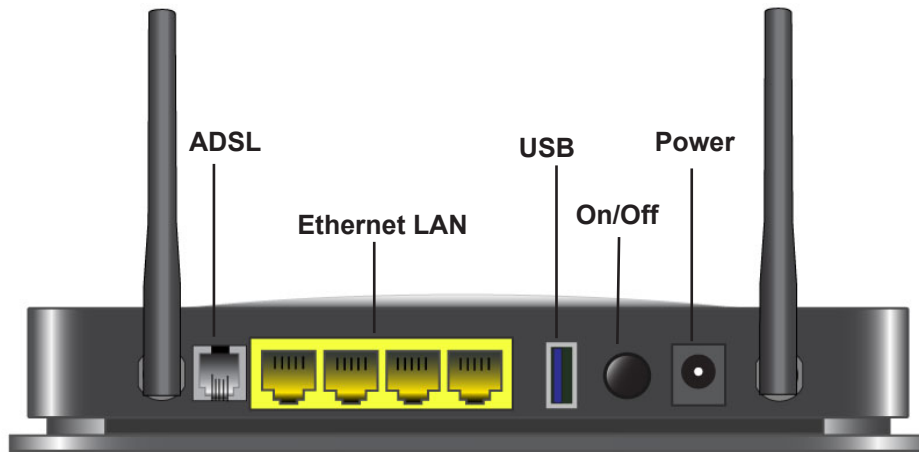
Figure 2. Back panel port connections

Front Panel

The modem router front panel has the status LEDs and icons shown in the figure. Note that the Wireless and WPS icons are buttons.

Power　　LAN Ports (1–4)　　USB　DSL　Internet　WiFi　WPS
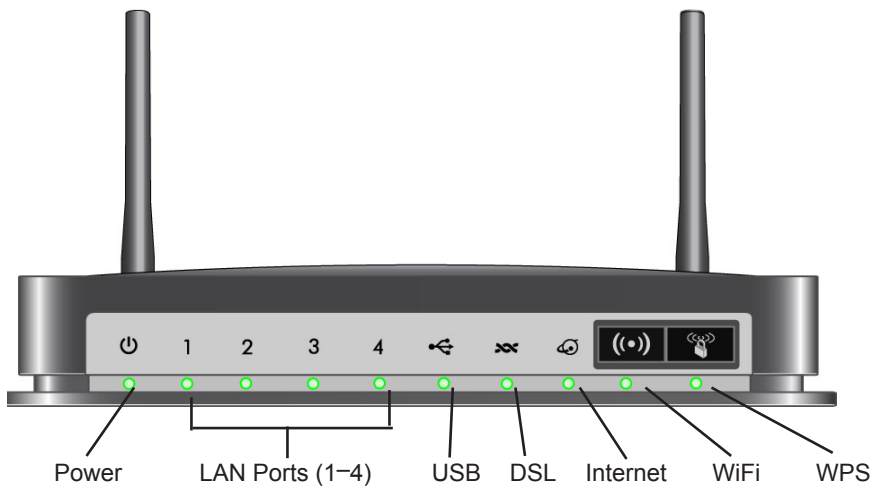
Figure 3. Front panel LEDs and icons

The following table describes the LEDs, icons, and buttons on the front panel from left to right.

Table 1. Front panel LEDs and buttons

Icon	Description
Power	• **Solid green**. Power is supplied to the modem router. • **Solid red**. POST (power-on self-test) failure or a device malfunction has occurred. • **Off**. Power is not supplied to the modem router. • **Blinking**. The LED blinks momentarily when the Restore Factory Settings button is pressed for 6 seconds (pressing it briefly resets the unit). The Power LED then blinks red three times when the Restore Factory Settings button is released and then turns green as the modem router resets to the factory defaults.
LAN	• **Solid green**. The LAN port has detected an Ethernet link with a device. • **Blinking green**.Data is being transmitted or received. • **Off**. No link is detected on this port.
USB	• **Solid green**. A USB device is connected and ready to use. • **Blinking green**. A USB device is in use. • **Off**. No USB device connected, or the Safely Remove Hardware" has been activated, or an error has occurred with the device.
DSL	• **Solid green**. You have a DSL connection. In technical terms, the DSL port is synchronized with an ISP's network-access device. • **Blinking green**. The modem router is negotiating the best possible speed on the DSL line. • **Off**. The unit is off or there is no DSL link established.
Internet	• **Solid green**. You have an Internet connection. If this connection is dropped due to an idle time-out but the DSL connection is still present, the LED stays green. If the Internet connection is dropped for any other reason, the LED turns off. • **Solid red**. The Internet (IP) connection failed. See *Troubleshooting the Internet Connection* on page 128 for troubleshooting information. • **Blinking green**. Data is being transmitted over the DSL port. • **Off**. No Internet connection is detected or the device is in bridge mode (an external device handles the ISP connection).
WiFi Icon is on the WiFi button	• **Solid green**. There is WiFi connectivity. • **Blinking green**. Data is being transmitted or received over the WiFi link. • **Off**. There is no WiFi connectivity. You can still plug an Ethernet cable into one of the LAN ports to get wired connectivity. See *Advanced Wireless Settings* on page 81 for more information about the use of this button.
WPS Icon is on the WPS button	• **Solid green**. Indicates that wireless security has been enabled. • **Blinking green**. A WPS-capable device is connecting to the device. • **Off**. WPS is not enabled. See *Wi-Fi Protected Setup (WPS) Method* on page 22 for more information about the use of this button.

Modem Router Stand

For optimal wireless network performance, use the stand (included in the package) to position your modem router upright.

1. Orient your modem router vertically.

2. Insert the tabs of the stand into the slots on the bottom of your modem router as shown.

3. Place your modem router in a suitable area for installation (near an AC power outlet and accessible to the Ethernet cables for your wired computers).

Position Your Modem Router

The modem router lets you access your network from virtually anywhere within the operating range of your wireless network. However, the operating distance or range of your wireless connection can vary significantly depending on the physical placement of your modem router. For example, the thickness and number of walls the wireless signal passes through can limit the range. For best results, place your modem router:

* Near the center of the area where your computers and other devices operate and preferably within line of sight to your wireless devices.

* So it is accessible to an AC power outlet and near Ethernet cables for wired computers.

* In an elevated location such as a high shelf, keeping the number of walls and ceilings between the modem router and your other devices to a minimum.

* Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, computers, or the base of a cordless phone or 2.4 GHz cordless phone.

- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

- With the antennas in a vertical position to provide the best side-to-side coverage or in a horizontal position to provide the best up-and-down coverage, as applicable.

When you use multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

ADSL Microfilters

If this is the first time you have cabled a router between a DSL phone line and your computer or laptop, you might not be familiar with ADSL microfilters. If you are, you can skip this section and proceed to *Cable Your Modem Router* on page 13.

An ADSL microfilter is a small inline device that filters DSL interference out of standard phone equipment that shares the same line with your DSL service. Every telephone device that connects to a telephone line that provides DSL service needs an ADSL microfilter to filter out the DSL interference. Examples of devices are telephones, fax machines, answering machines, and caller ID displays. Note that not every phone line in your home necessarily carries DSL service. That depends on the DSL service setup in your home.

> **Note:** Often the ADSL microfilter is in the box with the modem router. If you purchased the modem router in a country where a microfilter is not included, you have to acquire the ADSL microfilter separately.

One-Line ADSL Microfilter

Plug the ADSL microfilter into the wall outlet and plug your phone equipment into the jack labeled Phone. The modem router plugs directly into a separate DSL line. Plugging the modem router into the phone jack blocks the Internet connection. If you do not have a separate DSL line for the modem router, the best thing to do is to use an ADSL microfilter with a built-in splitter (see *Two-Line ADSL Microfilter* on page 13).

Plugs into DSL line

Figure 4. One-line ADSL microfilter

If you do not have a separate DSL line for the modem router, the second-best solution is to get a separate splitter. To use a one-line filter with a separate splitter, insert the splitter into the phone outlet, connect the one-line filter to the splitter, and connect the phone to the filter.

Two-Line ADSL Microfilter

Use an ADSL microfilter with a built-in splitter when there is a single wall outlet that provides connectivity for both the modem router and your telephone equipment. Plug the ADSL microfilter into the wall outlet, plug your phone equipment into the jack labeled Phone, and plug the modem router into the jack labeled ADSL.

Plugs into the DSL line

Figure 5. Two-line ADSL microfilter with built-in splitter

Summary

- One-line ADSL microfilter. Use with a phone or fax machine.
- Splitter. Use with a one-line ADSL microfilter to share an outlet with a phone and the modem router.
- Two-line ADSL microfilter with built-in splitter. Use to share an outlet with a phone and the modem router.

Cable Your Modem Router
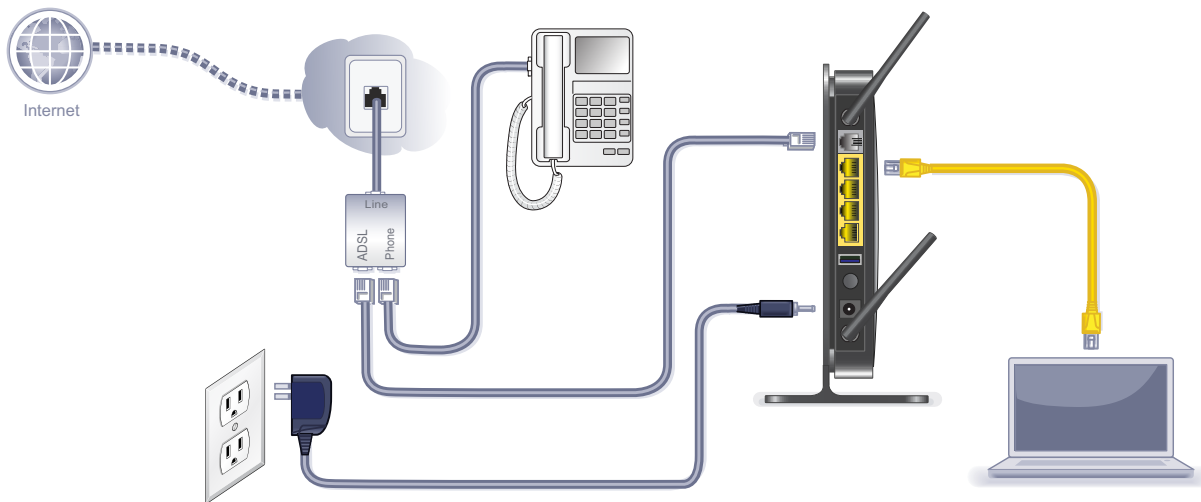
Figure 6. Cable connections

⚠️ **CAUTION:**

Incorrectly connecting a filter to your modem router blocks your DSL connection.

This section includes the same information about the printed installation guide that came with the modem router.

➢ **To cable the modem router:**

1. Connect the ADSL.

   a. Install an ADSL microfilter between the phone line and the phone.
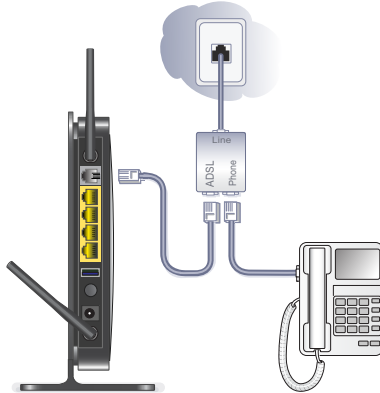
   b. Connect the ADSL port of the modem router to the ADSL port of the microfilter

   c. Use an ADSL microfilter for every phone line in the house if your modem router and telephone connect to the same phone line.

2. Add power to the modem router.
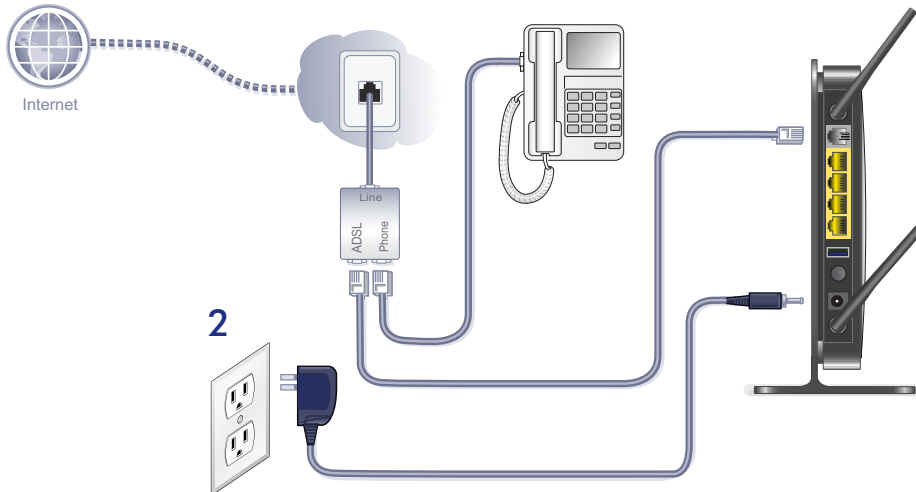
   a. Connect the power adapter to the router and plug the power adapter into an outlet.

   b. Wait for the WiFi LED on the front panel to turn on. If none of the LEDs on the front panel are on, press the **On/Off** button on the rear panel of the modem router.

3. Connect the computer.

You can use an Ethernet cable or connect wirelessly.
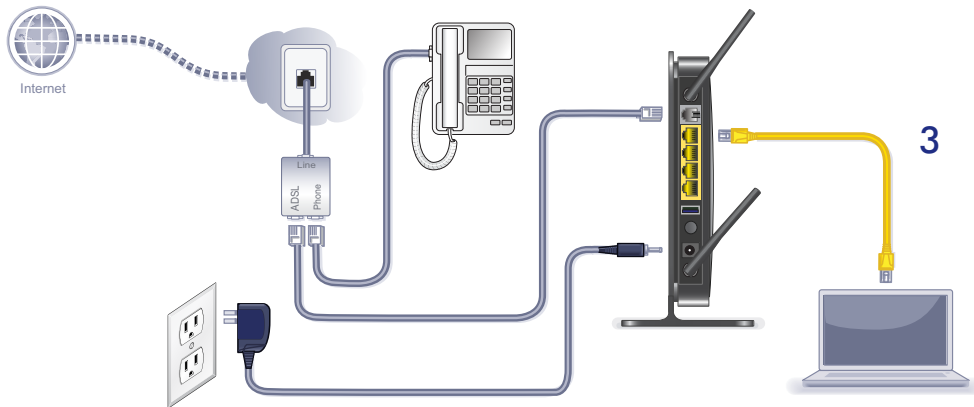
- Use the yellow Ethernet cable to connect your computer to an Ethernet port on your router.
- Or, connect wirelessly by using the preset wireless security settings located on the label on the bottom of the router.

4. Open a browser.
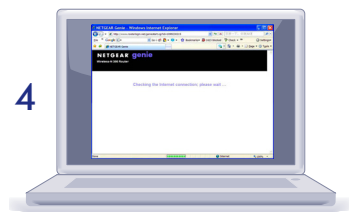
If a web page does not open, close and reopen the browser and enter **http://routerlogin.net** in the address bar.

5. Connect any additional wired computers to your modem router by inserting an Ethernet cable from a computer into one of the three remaining LAN ports.

Note: If you are an advanced user who wants to set up the modem to run in "pure bridge" or Modem mode, you need to log in to the modem and change the Device Mode setting to Modem mode. See *Change the Device Mode* on page 93.

Verify the Cabling

Verify that your modem router is cabled correctly by checking the modem router LEDs. Turn on the modem router by pressing the **On/Off** button on the back.

- ⏻ The Power LED is green when the modem router is turned on.
- ① The LAN ports are green for each computer cabled to the modem router by an Ethernet cable.
- The WiFi LED is green when the modem router is turned on.
- The DSL LED is green when you have a DSL connection.
- The Internet LED is red when there is no Internet connection.

Turn on your computer. If software usually logs you in to your Internet connection, do not run that software. Cancel it if it starts automatically.

Verify that the LAN ① LEDs (1 through 4) are lit for any computers cabled to the modem router by an Ethernet cable.

Getting Started with NETGEAR genie

2

Connecting to the modem router

This chapter explains how to use NETGEAR genie to set up your modem router after you complete cabling as described in the installation guide and in the previous chapter.

This chapter contains the following sections:

- *Modem Router Setup Preparation*
- *Types of Logins and Access*
- *NETGEAR genie Setup*
- *Use NETGEAR genie after Installation*
- *Upgrade the Firmware*
- *Dashboard (Basic Home Screen)*
- *Join Your Wireless Network*
- *NETGEAR genie App and Mobile genie App*

Modem Router Setup Preparation

You can set up your modem router with the NETGEAR genie automatically, or you can use the genie menus and screens to set up your modem router manually. Before you start the setup process, get your ISP information and make sure the computers and devices in the network have the settings described here.

Use Standard TCP/IP Properties for DHCP

If you set up your computer to use a static IP address, you need to change the settings so that it uses Dynamic Host Configuration Protocol (DHCP).

Gather ISP Information

If you have DSL broadband service, you might need the following information to set up your modem router and to check that your Internet configuration is correct. Your Internet service provider (ISP) should have provided you with all of the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it. When your Internet connection is working, you no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your modem router automatically logs you in. Make sure that you have the following information:

- The ISP configuration information for your DSL account
- ISP login name and password
- Fixed or static IP address settings (special deployment by ISP; this is rare)

Wireless Devices and Security Settings

Make sure that the wireless device or computer that you are using supports WPA or WPA2 wireless security, which is the wireless security supported by the modem router.

Types of Logins and Access

There are separate types of logins that have different purposes. It is important that you understand the difference so that you know which login to use when.

- **Modem Router login** logs you in to the modem router interface from NETGEAR genie. See *Use NETGEAR genie after Installation* on page 20 for details about this login.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **Wireless network key or password**. Your modem router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the label on the bottom of your modem router.

NETGEAR genie Setup

NETGEAR genie runs on any device with a web browser. Installation and basic setup takes about 15 minutes to complete.
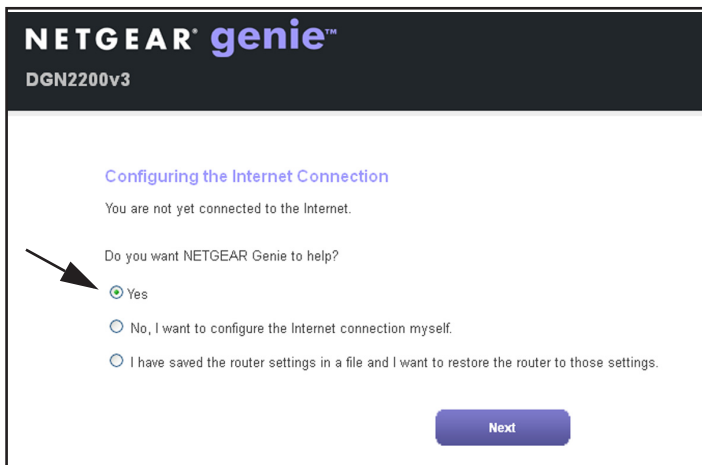
> **To use NETGEAR genie to set up your modem router:**

1. Turn the modem router on by pressing the **On/Off** button.

2. Make sure that your computer or wireless device is connected to the modem router with an Ethernet cable (wired) or wirelessly with the preset security settings listed on the bottom label.

3. Launch your Internet browser.
   - The first time you set up the Internet connection for your modem router, the browser goes to http://www.routerlogin.net and the NETGEAR genie screen displays.
   - If you already used the NETGEAR genie, type **http://www.routerlogin.net** in the address field for your browser to display the NETGEAR genie screen. See *Use NETGEAR genie after Installation* on page 20.

4. Follow the onscreen instructions to complete NETGEAR genie setup. NETGEAR genie guides you through connecting the modem router to the Internet.

If the browser cannot display the web page:

- Make sure that the computer is connected to one of the four LAN Ethernet ports or wirelessly to the modem router.

- Make sure that the router has full power, and that its wireless LED is lit.

- Close and reopen the browser to make sure that the browser does not cache the previous page.

- Browse to **http://www.routerlogin.net.**

- If the computer is set to a static or fixed IP address (this is uncommon), change it to obtain an IP address automatically from the modem router.

If the modem router does not connect to the Internet:

1. Review your settings to be sure that you have selected the correct options and typed everything correctly.

2. Contact your ISP to verify that you have the correct configuration information.

3. Read *Chapter 10, Troubleshooting*. If problems persist, register your NETGEAR product and contact NETGEAR technical support.

Use NETGEAR genie after Installation

When you first set up your modem router, NETGEAR genie automatically starts when you launch an Internet browser on a computer that is connected to the modem router. You can use NETGEAR genie again if you want to view or change settings for the modem router.

1. Launch your browser from a computer or wireless device that is connected to the modem router.

2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

   The login window displays:

User name:	🔒 admin	∨
Password:	********	
	☐ Remember my password	
	OK Cancel	

3. Enter **admin** for the modem router user name and **password** for the modem router password, both in lowercase letters.

   Note: *The modem router user name and password are different from the user name and password for logging in to your Internet connection. See* Types of Logins and Access *on page 18 for more information.*

Upgrade the Firmware

When you set up your modem router and are connected to the Internet, the modem router automatically checks for you to see if newer firmware is available. If it is, a message is displayed on the top of the screen. See *Upgrade the Modem Router Firmware* on page 73 for more information about upgrading firmware.

Click the message when it shows up and click **Yes** to upgrade the modem router with the latest firmware. After the upgrade, the modem router restarts.

> ⚠️ **CAUTION:**
>
> Do not try to go online, turn off the modem router, shut down the computer, or do anything else to the modem router until the modem router finishes restarting and the Power LED has stopped blinking for several seconds.

Dashboard (Basic Home Screen)

The modem router Basic Home screen has a dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the six sections of the dashboard to view more detailed information. The left column has the menus, and at the top, there is an Advanced tab that you can use to access additional menus and screens.
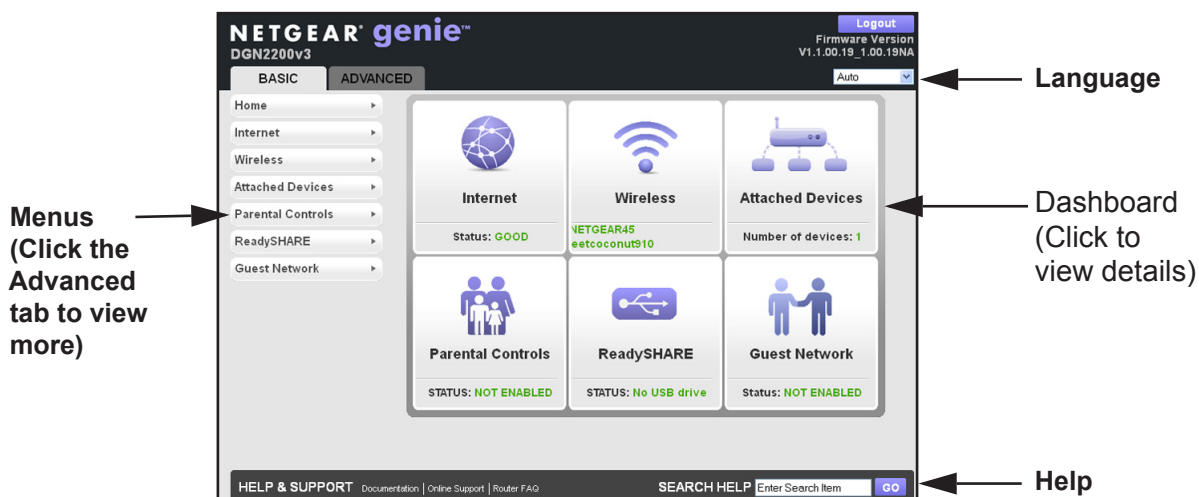
Figure 7. Basic Home screen with dashboard, language, and online help

- **Home. This dashboard screen displays when you log in to the** modem router**.**
- **Internet**. Set, update, and check the ISP settings of your modem router.
- **Wireless**. View or change the wireless settings for your modem router.
- **Attached Devices**. View the devices connected to your network.
- **Parental Controls**. Download and set up parental controls to prevent objectionable content from reaching your computers.

- **ReadySHARE**. If you connected a USB storage device to the modem router, then it is displayed here.

- **Guest Network**. Set up a guest network to allow visitors to use your modem router's Internet connection.

- **Advanced tab**. Set the modem router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Chapter 8, Advanced Settings*. You need a solid understanding of networking protocols to use this tab.

- **Help & Support**. Go to the NETGEAR support site to get information, help, and product documentation. These links work once you have an Internet connection.

Join Your Wireless Network

You can use the manual or the WPS method to join your wireless network. See *Guest Networks* on page 35 for instructions about how to set up a guest network.

Manual Method

With the manual method, choose the network that you want and type its password to connect.

➢ **To connect manually:**

1. On your computer or wireless device, open the software that manages your wireless connections. This software scans for all wireless networks in your area.

2. Look for your network and select it.

   The unique WiFi network name (SSID) and password is on the router label. If you changed these settings, then look for the network name that you used.

3. Enter the modem router password and click **Connect**.

Wi-Fi Protected Setup (WPS) Method

Wi-Fi Protected Setup (WPS) lets you connect to a secure WiFi network without typing its password. Instead, press a button or enter a PIN. NETGEAR calls WPS Push 'N' Connect.

Some older WiFi equipment is not compatible with WPS. WPS works only with WPA2 or WPA wireless security.

➢ **To use WPS to join the wireless network:**

1. Press the **WPS** button on the modem router front panel .

2. Within 2 minutes, press the **WPS** button on your wireless device or follow the WPS instructions that came with the device.

   The WPS process automatically sets up your wireless computer with the network password and connects you to the wireless network.

NETGEAR genie App and Mobile genie App

The genie app is the easy dashboard for managing, monitoring, and repairing your home network. See the NETGEAR genie App User Manual for details about the genie apps.

The genie app can help you with the following:

- Automatically repair common wireless network problems.
- Have easy access to router features like Live Parental Controls, guest access, Internet traffic meter, speed test, and more.

The genie mobile app works on your iPhone, iPad, or Android phone:
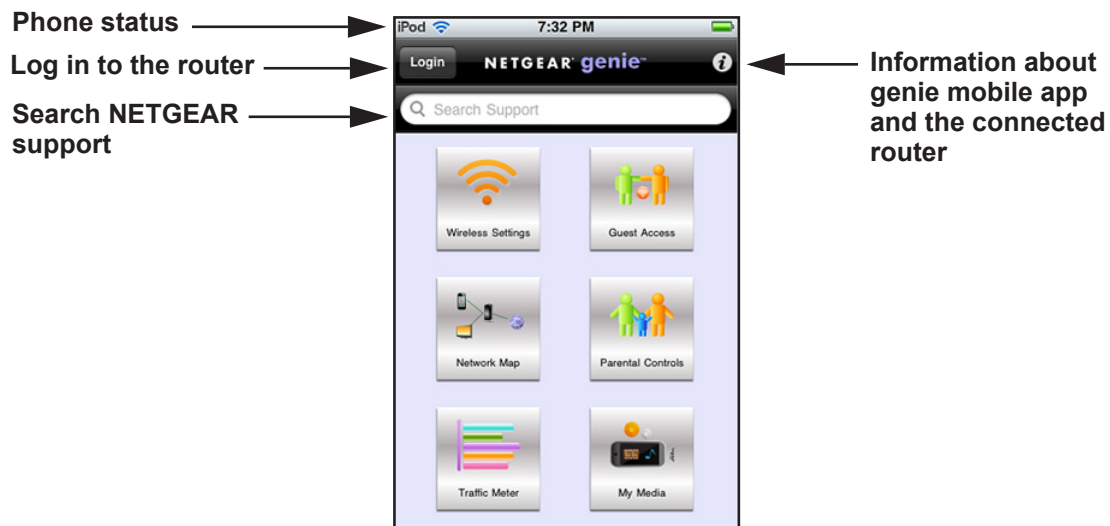
NETGEAR genie Basic Settings

3

Your Internet connection and network

This chapter contains the following sections:

- *Basic Home Screen*
- *Internet Setup*
- *Attached Devices*
- *Parental Controls*
- *ReadySHARE USB Storage*
- *Basic Wireless Settings*

Basic Home Screen

The genie Basic Home screen is shown in the following figure:

Internet Setup

The Internet Setup screen is where you view or change basic ISP information.

Note: You can use the Setup Wizard to detect the Internet connection and automatically set up the modem router. See *Setup Wizard* on page 38.

➢ **To view or change the basic Internet setup:**

1. From the Home screen, select **Internet**. The following screen displays:

The fields that display in the Internet Setup screen depend on whether your Internet connection requires a login.

- **Yes**. Select the encapsulation method and enter the login name. If you want to change the login time-out, enter a new value in minutes.

- **No**. Enter the account and domain names, only if needed.

2. Enter the settings for the IP address and DNS server. The default settings usually work fine. If you have problems with your connection, check the ISP settings.

3. Click **Apply** to save your settings.

4. Click **Test** to test your Internet connection. If the NETGEAR website does not display within 1 minute, see *Chapter 10, Troubleshooting*.

Internet Setup Screen Fields

The following descriptions explain all of the possible fields in the Internet Setup screen. The fields that display in this screen depend on whether tan ISP login is required.

Does Your ISP Require a Login? Answer either yes or no.

These fields display when no login is required:

- **Account Name (If required)**. Enter the account name provided by your ISP. This might also be called the host name.

- **Domain Name (If required)**. Enter the domain name provided by your ISP.

These fields display when your ISP requires a login:

- **Internet Service Provider Encapsulation**. ISP types. The choices are PPPoE, PPTP, or L2TP.

- **Login**. The login name provided by your ISP. This login name is often an email address.

- **Password**. The password that you use to log in to your ISP.
- **Idle Timeout (In minutes)**. If you want to change the login timeout, enter a new value in minutes. This setting determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. A value of 0 (zero) means never log out.

Internet IP Address.

- **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
- **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's modem router to which your modem router will connect.

Domain Name Server (DNS) Address. The DNS server is used to look up site addresses based on their names.

- **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
- **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

Modem Router MAC Address. The Ethernet MAC address that the modem router uses on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They accept traffic only from the MAC address of that computer. This feature allows your modem router to use your computer's MAC address (this is also called cloning).

- **Use Default Address**. Use the default MAC address.
- **Use Computer MAC Address**. The modem router captures and uses the MAC address of the computer that you are now using. You have to use the one computer that is allowed by the ISP.
- **Use This MAC Address**. Enter the MAC address that you want to use.

Attached Devices

Use the Attached Device screen to view all computers or devices that are currently connected to your network.

➢ **To go to the Attached Devices screen:**

From the Basic Home screen, select **Attached Devices** to display the following screen:

Wired devices are connected to the modem router with Ethernet cables. Wireless devices have joined the wireless network.

- **#** (number). The order in which the device joined the network.
- **IP Address**. The IP address that the modem router assigned to this device when it joined the network. This number can change if a device is disconnected and rejoins the network.
- **Device Name**. If the device name is known, it is shown here.
- **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label.

You can click **Refresh** to update this screen.

Parental Controls

The first time you select Parental Controls from the Basic Home screen, your browser goes to the Parental Controls website. You can learn more about Live Parental Controls or download the application.
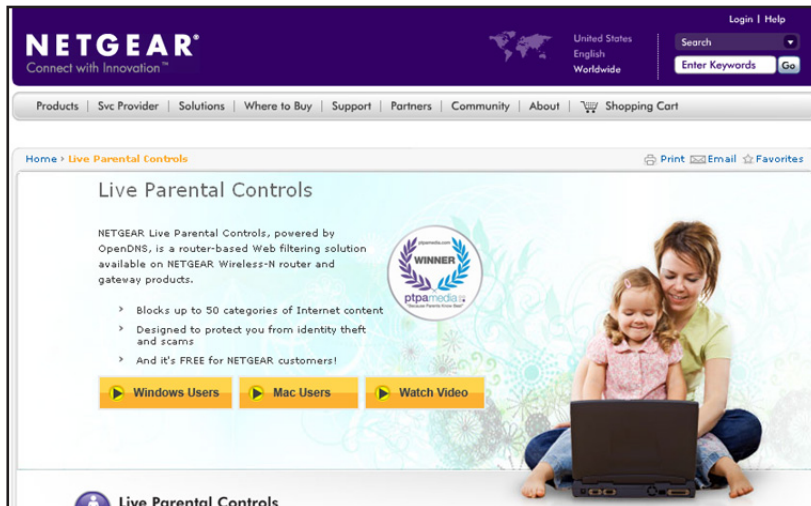
> ➢ **To set up Live Parental Controls:**

1. Select **Parental Controls** on the Dashboard screen.

2. Click either the **Windows Users** or **Mac Users** button.

3. Follow the onscreen instructions to download and install the NETGEAR Live Parental Controls Management Utility.

    After installation, Live Parental Controls automatically starts.
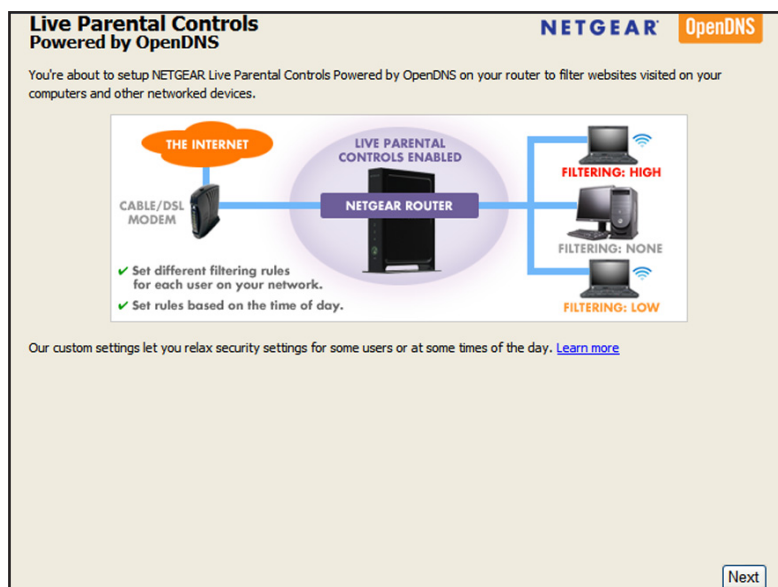
4. Click **Next**, read the note, and click **Next** again to proceed.

Because Live Parental Controls uses free OpenDNS accounts, you are prompted to log in or create a free account.

Setting up Live Parental Controls

Welcome, this setup wizard will quickly configure NETGEAR Live Parental Controls Powered by OpenDNS on your NETGEAR router.

In order to use Live Parental Controls, you need a free OpenDNS account. Do you already have one?

⦿ Yes, use my existing OpenDNS account.
○ No, I need to create a free OpenDNS account.

5. Select the radio button that applies to you and click **Next**.
   - If you already have an OpenDNS account, leave the **Yes** radio button selected.
   - If you do not have an OpenDNS account, select the **No** radio button.

   If you are creating an account, the following screen displays:

   Create a free OpenDNS account

Username		Check availability
Password	
Confirm Password	
Email	
Confirm Email	

   - Fill in the fields and click **Next**.

   After you log on or create your account, the filtering level screen displays:

   Live Parental Controls: choose a filtering level for your network

   All computers connected to your router will be protected from the content you select below. You can customize your Live Parental Controls later on our website.

   ○ **High**
   Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, phishing attacks and general time-wasters.

   ○ **Moderate**
   Protects against all adult-related sites, illegal activity and phishing attacks.

   ○ **Low**
   Protects against pornography and phishing attacks.

   ⦿ **Minimal**
   Protects only against phishing attacks.

   ○ **None**
   Nothing blocked.

6. Select the radio button for the filtering level that you want and click **Next**.

Setup is complete!

You have successfully setup NETGEAR Live Parental Controls Powered by OpenDNS. Next time you run the Management Utility it will take you to the status screen where you can:

- check whether Live Parental Controls are enabled
- disable or enable Live Parental Controls
- modify basic settings
- change custom settings such as per-user and time-of-day based Live Parental Controls

Take me to the status screen

7. Click the T**ake me to the status screen** button.

Parental controls are now set up for the router. The Dashboard shows Parental Controls as Enabled.

ReadySHARE USB Storage

You can view information about a USB storage device that is connected to the modem router's USB port here. From the Basic Home screen, select **ReadySHARE** to display the USB Storage (Basic Settings) screen:

USB Storage (Basic Settings)

- Basic
- ReadySHARE Printer

Network/Device Name \\readyshare

Available Network Folders

Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space

Edit

Safely Remove USB Device

Refresh

This screen displays the following:

- **Network/Device Name**. The default is \\readyshare. This is the name used to access the USB device connected to the modem router.

- **Available Network Folders**. The folders on the USB device.

  Share Name. If only one device is connected, the default share name is USB_Storage. You can click the name shown, or you can type it in the address field of your web browser. If Not Shared is shown, the default share has been deleted, and no other share for the root folder exists. Click the link to change this setting.

  Read/Write Access. Shows the permissions and access controls on the network folder: All – no password (the default) allows all users to access the network folder. The user

name (account name) for All – no password is guest. The password for **admin** is the same one that you use to log in to the modem router. By default, it is **password**.

Folder Name. Full path of the network folder.

Volume Name. Volume name from the storage device (either USB drive or HDD).

Total/Free Space. Shows the current utilization of the storage device.

- **Edit**. Click the **Edit** button to edit the Available Network Folders settings.
- **Safely Remove a USB Device**. Click to safely remove the USB device attached to your modem router.

You can click **Refresh** to update this screen.

For more information about USB storage, see *Chapter 5, USB Storage*.

Basic Wireless Settings

The Wireless Settings screen lets you view or configure the wireless network setup.

The N300 Wireless ADSL2+ Modem Router comes with preset security. This means that the Wi-Fi network name (SSID), network key (password), and security option (encryption protocol) are preset in the factory. You can find the preset SSID and password on the bottom of the unit.

> **Note:** The preset SSID and password are uniquely generated for every device to protect and maximize your wireless security.

➢ **To view or change basic wireless settings:**

NETGEAR recommends that you do not change your preset security settings. If you change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

If you use a wireless computer to change the wireless network name (SSID) or other wireless security settings, you are disconnected when you click Apply. To avoid this problem, use a computer with a wired connection to access the modem router.

1. Select **Basic > Wireless** to display the Wireless Settings screen.

The screen sections, settings, and procedures are explained in the following sections.

2. Make any changes that are needed and click **Apply** to save your settings.

3. Set up and test your wireless devices and computers to make sure that they can connect wirelessly. If they do not, check the following:

   • Is your wireless device or computer connected to your network or another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.

   • Does your wireless device or computer show up on the Attached Devices screen? If it does, then it is connected to the network.

   • If you are not sure what the network name (SSID) or password is, look on the label on the bottom of your modem router.

Wireless Settings Screen Fields

Region Selection

The location where the modem router is used. Select from the countries in the list. In the United States, the region is fixed to United States and is not changeable.

Wireless Network (2.4 GHz b/g/n)

The b/g/n notation references the 802.11 standards of conformance for the 2.4 GHz radio frequency.

Enable Wireless Isolation. If this check box is selected, computers or wireless devices that join the network can use the Internet, but cannot access each other or access Ethernet devices on the network.

Enable SSID Broadcast. This setting allows the modem router to broadcast its SSID so wireless stations can see this wireless name (SSID) in their scanned network lists. This

check box is selected by default. To turn off the SSID broadcast, clear the **Allow Broadcast of Name (SSID)** check box, and click **Apply**.

Name (SSID). The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and *NETGEAR strongly recommends that you do not change this setting.*

Channel. This setting is the wireless channel the gateway uses. Enter a value from 1 through 13. (For products in the North America market, only Channels 1 through 11 can be operated.) Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

- **Mode**. Up to 150 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. Up to 65 Mbps supports up to 65 Mbps.

Security Options Settings

The Security Options section of the Wireless Settings screen lets you change the security option and passphrase. ***NETGEAR recommends that you do not change the security option or passphrase,*** but if you want to change these settings, this section explains how. ***Do not disable security***.

Change WPA Security Option and Passphrase

You can change the security settings for your modem router. If you do so, then write down the new settings and store them in a secure place for future reference.

➢ **To change the WPA settings:**

1. On the Wireless Settings screen, under Security Options, select the WPA option you want.
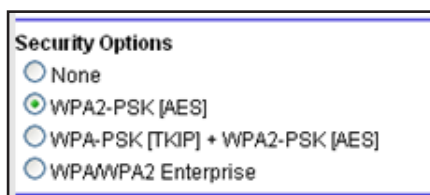
2. In the Passphrase field that displays when you select a WPA security option, enter the network key (passphrase) that you want to use. It is a text string from 8 to 63 characters.

Guest Networks

Adding a guest network allows visitors at your home to use the Internet without giving them your wireless security key. You can add a guest network to each wireless network: 2.4 GHz b/g/n and 5.0 GHz a/n.

➢ **To set up a guest network:**

1. Select **Basic > Guest Network** to display the following screen:

2. Select any of the following wireless settings:

   Enable this wireless network. When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile.

   Enable SSID Broadcast. If this check box is selected, the wireless access point broadcasts its name (SSID) to all wireless stations. Stations with no SSID can adopt the correct SSID for connections to this access point.

   Allow guest to access My Local Network. If this check box is selected, anyone who connects to this SSID has access to your local network, not just Internet access.

   Enable Wireless Isolation. If this check box is selected, wireless computers or devices that join the network can use the Internet but cannot access each other or access Ethernet devices on the network.

3. Give the guest network a name.

   The guest network name is case-sensitive and can be up to 32 characters. You then manually configure the wireless devices in your network to use the guest network name in addition to the main SSID.

4. Select a security option from the list. The security options are described in *Guest Network Wireless Security Options* on page 36.

5. Click **Apply** to save your selections.

Guest Network Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. Wi-Fi Protected Access (WPA) has several options including pre-shared key (PSK) encryption.

This section presents an overview of the security options and provides guidance on when to use which option. It is also possible to set up a guest network without wireless security. NETGEAR does *not* recommend this.

WPA Encryption

WPA encryption is built into all hardware that has the Wi-Fi-certified seal. This seal means that the product is authorized by the Wi-Fi Alliance (*http://www.wi-fi.org/*) because it complies with the worldwide single standard for high-speed wireless local area networking.

WPA uses a passphrase for authentication and to generate the initial data encryption keys. Then it dynamically varies the encryption key. WPA-PSK uses Temporal Key Integrity Protocol (TKIP) data encryption, implements most of the IEEE 802.11i standard, and works with all wireless network interface cards, but not all wireless access points.

WPA2-PSK is stronger than WPA-PSK. It is advertised to be theoretically indecipherable due to the greater degree of randomness in encryption keys that it generates. WPA2-PSK gets higher speed because it is usually implemented through hardware, while WPA-PSK is usually implemented through software. WPA2-PSK uses a passphrase to authenticate and generate the initial data encryption keys. Then it dynamically varies the encryption key.

WPS-PSK + WPA2-PSK Mixed Mode can provide broader support for all wireless clients. WPA2-PSK clients get higher speed and security, and WPA-PSK clients get decent speed and security. For help with WPA settings on your wireless computer or device, see the instructions that came with your product.

NETGEAR genie Advanced Home

4

Specifying custom settings

This chapter contains the following sections:

- *NETGEAR genie Advanced Home Screen*
- *Setup Wizard*
- *WPS Wizard*
- *Setup Menu*
- *WAN Setup*
- *LAN Setup*
- *Quality of Service (QoS) Setup*

Some selections on the Advanced Home screen are described in separate chapters:

- **USB Storage**. See *Chapter 5, USB Storage*.
- **Security**. See *Chapter 6, Security*.
- **Administration**. See *Chapter 7, Administration*.
- **Advanced Setup**. See *Chapter 8, Advanced Settings*.
- **Advanced VPN**. See *Chapter 9, Virtual Private Networking*.

NETGEAR genie Advanced Home Screen

The genie Advanced Home dashboard presents status information. The content is the same as what is on the Router Status screen available from the Administration menu.The genie Advanced Home screen is shown in the following figure:
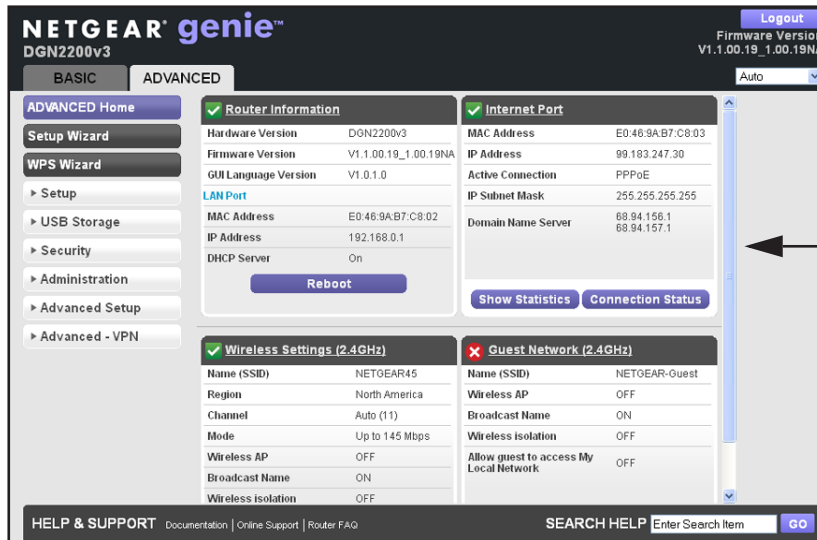
This screen is also displayed through the Administration menu.

Setup Wizard

You can use the Setup Wizard to detect your Internet settings and automatically set up your router. The Setup Wizard is not the same as the genie screens that display the first time you connect to your router to set it up.

➢ **To use the Setup Wizard:**

1. Select **Advanced > Setup Wizard** to display the following screen:
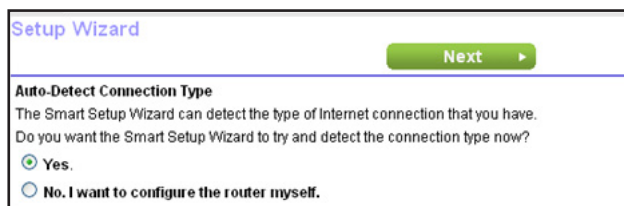
2. Select either **Yes** or **No, I want to configure the router myself**. If you select No, you are taken to the Internet Setup screen (see *Internet Setup* on page 25).

3. Select Yes and click **Next**.

> **Detecting the Internet Connection**
> This process can take up to six minutes; please wait ...

The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration. The following screen displays:

> **Congratulations!**
> You are successfully connected to the Internet.
> This router is preset with the following unique wireless network name (SSID) and network key (password)
>
> 2.4GHz Wireless Network Name (SSID) **NETGEAR35**
>
> 5GHz Wireless Network Name (SSID)   **NETGEAR35-5G**
>
> Wireless Network Key (Password)   **fuzzyumbrella906**
>
> [**Print this**]   [**Take me to the Internet**]
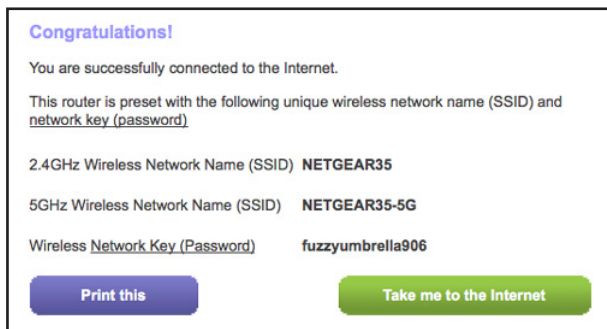
WPS Wizard

The WPS Wizard helps you add a WPS-capable client device (a wireless device or computer) to your network. On the client device, either press its WPS button or locate its WPS PIN.

➢ **To use the WPS Wizard:**

1. Select **Advanced > WPS Wizard**.

2. Click **Next**. The following screen lets you select the method for adding the WPS client (a wireless device or computer).

> **Add WPS Client**
>
> Select a setup method:
> ⦿ Push Button (recommended)
>   You can either press the physical push button on the router or click the button (soft push button) in this screen.
>
> ○ PIN Number
>   This is the security PIN of the WPS client. While connecting, WPS-enabled adapters provide a randomly-generated security PIN.
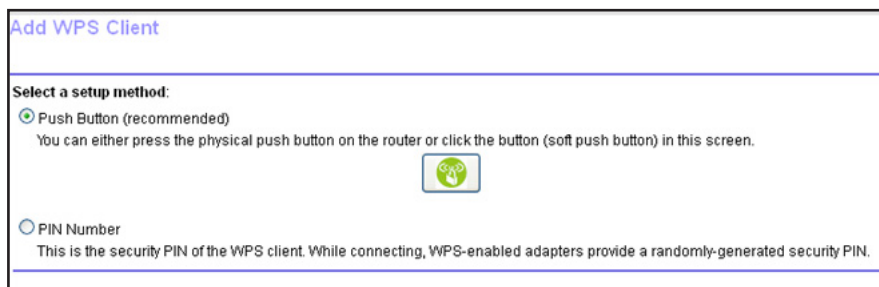
You can use either the push button or PIN method.

3. Select either **Push Button** or **PIN Number**.

   • To use the push button method, either click the **WPS** button on this screen, or press the **WPS** button on the side of the modem router. Within 2 minutes, go to the wireless client and press its **WPS** button to join the network without entering a password.

- To use the PIN method, select the **PIN Number** radio button, enter the client security PIN, and click **Next**.

Within 2 minutes, go to the client device and use its WPS software to join the network without entering a password.

The modem router attempts to add the WPS-capable device. The WPS LED on the front of the modem router blinks green. When the modem router establishes a WPS connection, the LED is solid green, and the modem router WPS screen displays a confirmation message.

4. Repeat Step 2 and Step 3 to add another WPS client to your network.

Setup Menu

Select **Advanced > Setup** to display the Setup menu. The following selections are available:

- **Internet Setup**. Go to the same Internet Setup screen that you can access from the dashboard on the Basic Home screen. See *Internet Setup* on page 25.
- **Wireless Setup**. Go to the same Wireless Settings screen that you can access from the dashboard on the Basic Home screen. See *Basic Wireless Settings* on page 32.
- **Guest Network**. This selection is a shortcut to the same Guest Network screen that you can access from the dashboard on the Basic Home screen. See *Guest Networks* on page 35.
- **WAN Setup**. Internet (WAN) setup. See *WAN Setup* on page 41.
- **LAN Setup**. Local area network (LAN) setup. See *LAN Setup* on page 44.
- **QoS Setup**. Quality of Service (QoS) setup. See *Quality of Service (QoS) Setup* on page 47.

WAN Setup

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the Maximum Transmit Unit (MTU) size, and enable the modem router to respond to a ping on the WAN (Internet) port.

➢ **To view or change the WAN settings:**

Select **Advanced > Setup > WAN Setup**

The following settings are available:

- **Disable Port Scan and DoS Protection**. DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. This should be disabled only in special circumstances.

- **Default DMZ Server**. This feature is sometimes helpful when you are playing online games or videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See the following section, *Default DMZ Server*, for more details.

- **Respond to Ping on Internet Port**. If you want the modem router to respond to a ping from the Internet, select this check box. Use this setting only as a diagnostic tool because it allows your modem router to be discovered. Do not select this check box unless you have a specific reason.

- **MTU Size (in bytes)**. The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs, you might need to reduce the MTU. This is rarely required. You should only change the setting in this field if you are sure it is necessary for your ISP connection. See *Change the MTU Size* on page 42.

- **NAT Filtering**. Network Address Translation (NAT) determines how the modem router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. Open

NAT provides a much less secured firewall, but allows almost all Internet applications to function.

- **Disable SIP ALG**. The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. The Disable SIP ALG check box allows you to disable the SIP ALG. Disabling the SIP ALG might be useful when running certain applications.

- **Disable IGMP Proxying**. The IGPM Proxying feature lets a LAN computer receive the multicast traffic directed to it from the Internet. Selecting this check box prevents this from occurring.

Default DMZ Server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The modem routerrecognizes some of these applications and works correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

⚠️ **WARNING:**

> **DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.**

The router usually detects and discards Incoming traffic from the Internet that is not a response to one of your local computers or a service that you have set up in the Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can have the router forward the traffic to one computer on your network. This computer is called the default DMZ server.

➢ **To set up a default DMZ server:**

1. On the WAN Setup screen, select the **Default DMZ Server** check box.
2. Type the IP address.
3. Click **Apply**.

Change the MTU Size

The Maximum Transmission Unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If a device in the data path has a lower MTU setting than the other devices, the data packets are split or "fragmented" to accommodate the device with the smallest MTU.

The best MTU setting for NETGEAR equipment is often just the default value. In some situations, changing the value fixes one problem but causes another. Leave the MTU unchanged unless one of these situations occurs:

- You have problems connecting to your ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications might require an MTU change:
  - A secure website that does not open, or displays only part of a web page
  - Yahoo email
  - MSN portal
  - America Online's DSL service
- You use VPN and have severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.

> **Note:** An incorrect MTU setting can cause Internet communication problems. For instance, you might not be able to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. The following table describes common MTU sizes and applications.

Table 2. Common MTU Sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This setting is typical for connections that do not use PPPoE or VPN, and is the default value for NETGEAR modem routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

➢ **To change the MTU size:**

1. Select **Advanced > Setup > WAN Setup**.
2. In the MTU Size field, enter a value from 64 to 1500.
3. Click **Apply** to save the settings.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

The modem router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The modem router's default LAN IP configuration is:

- LAN IP address. **192.168.1.1**
- Subnet mask. **255.255.255.0**

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. If your network requires a different IP addressing scheme, you can change these settings in the LAN Setup screen.

➢ **To change the LAN settings:**

Note: If you change the LAN IP address of the modem router while connected through the browser, you will be disconnected. You will have to open a new connection to the new IP address and log in again.

---

1. Select **Advanced > Setup > LAN Setup** to display the following screen:

2. Enter the settings that you want to customize. These settings are described in the following section, *LAN Setup Screen Settings*.

3. Click **Apply** to save your changes.

LAN Setup Screen Settings

LAN TCP/IP Setup

- **IP Address**. The LAN IP address of the modem router.

- **IP Subnet Mask**. The LAN subnet mask of the modem router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which addresses have to be reached through a gateway or modem router.

- **RIP Direction**. Router Information Protocol (RIP) allows a router to exchange routing information with other routers. This setting controls how the router sends and receives RIP packets. Both is the default setting. With the Both or Out Only setting, the router broadcasts its routing table periodically. With the Both or In Only setting, the router incorporates the RIP information that it receives.

- **RIP Version**. This setting controls the format and the broadcasting method of the RIP packets that the modem router sends. It recognizes both formats when receiving. By default, the RIP function is disabled.

  RIP-1 is universally supported. It is adequate for most networks, unless you have an unusual network setup.

  RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.

Use Router as a DHCP Server

Usually, this check box is selected so that the modem router functions as a Dynamic Host Configuration Protocol (DHCP) server.

- **Starting IP Address**. Specify the start of the range for the pool of IP addresses in the same subnet as the modem router.

- **Ending IP Address**. Specify the end of the range for the pool of IP addresses in the same subnet as the modem router.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it accesses the modem router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings. See *Address Reservation* on page 46.

Use the Modem Router as a DHCP Server

By default, the modem router acts as a DHCP server. The router assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the modem router. The modem router assigns IP addresses to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. For most applications, the default DHCP and TCP/IP settings of the modem router are satisfactory.

You can specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the modem router's LAN IP address. Using the default addressing scheme, define a range between 192.168.1.2 and 192.168.1.254, although you might want to save part of the range for devices with fixed addresses.

The modem router delivers the following parameters to any LAN device that requests DHCP:

* An IP address from the range that you have defined
* Subnet mask
* Gateway IP address (the modem router's LAN IP address)
* DNS server IP address (the modem router's LAN IP address)

To use another device on your network as the DHCP server, or to specify the network settings of all of your computers, clear the **Use Router as DHCP Server** check box and click **Apply**. Otherwise, leave this check box selected. If this service is not enabled and no other DHCP server is available on your network, set your computers' IP addresses manually so that they can access the modem router.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the modem router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

➢ **To reserve an IP address:**

1. In the Address Reservation section of the screen, click the **Add** button.
2. In the IP Address field, type the IP address to assign to the computer or server. (Choose an IP address from the modem router's LAN subnet, such as 192.168.1.x.)
3. Type the MAC address of the computer or server.

   Tip: If the computer is already on your network, you can copy its MAC address from the Attached Devices screen and paste it here.

4. Click **Apply** to enter the reserved address into the table.

The reserved address is not assigned until the next time the computer contacts the modem router's DHCP server. Reboot the computer, or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry, select the radio button next to the reserved address you want to edit or delete. Then click **Edit** or **Delete**.

Quality of Service (QoS) Setup

QoS is an advanced feature that can be used to prioritize some types of traffic ahead of others. The N300 Wireless ADSL2+ Modem Router can provide QoS prioritization over the wireless link and on the Internet connection.

➢ **To configure QoS:**

Select **Advanced > Setup > QoS Setup** to display the following screen:

Enable WMM QoS for Wireless Multimedia Applications

The N300 Wireless ADSL2+ Modem Router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application have to have WMM enabled. Legacy applications that do not support WMM and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video.

WMM QoS is enabled by default. You can disable it in the QoS Setup screen by clearing the **Enable WMM** check box and clicking **Apply**.

Set Up QoS for Internet Access

You can give prioritized Internet access to the following types of traffic:

- Specific applications
- Specific online games

- Individual Ethernet LAN ports of the modem router
- A specific device by MAC address

To specify prioritization of traffic, create a policy for the type of traffic and add the policy to the QoS Policy table in the QoS Setup screen. For convenience, the QoS Policy table lists many common applications and online games that can benefit from QoS handling.

QoS for Applications and Online Gaming

➢ **To create a QoS policy for applications and online games:**

1. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
2. Click the **Setup QoS Rule** button to see the QoS Priority Rule list.

You can edit or delete a rule by selecting its radio button and clicking either the **Edit** or **Delete** button. You can also delete all the rules by clicking the **Delete All** button.

3. To add a priority rule, scroll down to the bottom of the QoS Setup screen and click **Add Priority Rule** to display the following screen:

4. In the QoS Policy for field, type the name of the application or game.
5. In the Priority Category list, select either **Applications** or **Online Gaming**. In either case, a list of applications or games displays in the list.

6. You can select an existing item from the list, or you can scroll and select **Add a New Application** or **Add a New Game,** as applicable.

7. If prompted, in the Connection Type list, select either **TCP, UDP,** or both (**TCP/UDP**). Specify the port number or range of port numbers that the application or game uses.

8. From the Priority list, select the priority for Internet access for this traffic relative to other applications and traffic. The options are Low, Normal, High, and Highest.

9. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

QoS for a Modem Router LAN Port

➢ **To create a QoS policy for a device connected to one of the modem router's LAN ports:**

1. Select **Advanced > Setup > QoS Setup** to display the QoS Setup screen.

2. Select the **Turn Internet Access QoS On** check box.

3. Click the **Setup QoS Rule** button.

4. Click the **Add Priority Rule** button.

5. From the Priority Category list, select **Ethernet LAN Port**, as shown in the following figure:

6. From the LAN port list, select the LAN port.

7. From the Priority list, select the priority for Internet access for this port's traffic relative to other applications. The options are Low, Normal, High, and Highest.

8. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

9. In the QoS Setup screen, click **Apply**.

QoS for a MAC Address

➢ **To create a QoS policy for traffic from a specific MAC address:**

1. Select **Advanced > Setup > QoS Setup**, and click the **Setup QoS Rule** button. The QoS Setup screen displays.

2. Click **Add Priority Rule**.

3. From the Priority Category list, select **MAC Address** to display the following screen:

4. If the device to be prioritized appears in the MAC Device List, select its radio button. The information from the MAC Device List populates the policy name, MAC Address, and Device Name fields. If the device does not appear in the MAC Device List, click **Refresh**. If it still does not appear, then fill in these fields manually.

5. From the Priority list, select the priority for Internet access for this device's traffic reelative to other applications and traffic. The options are Low, Normal, High, and Highest.

6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

7. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.

8. Click **Apply**.

Edit or Delete an Existing QoS Policy

➢ **To edit or delete a QoS policy:**

1. Select **Advanced > QoS Setup** to display the QoS Setup screen.

2. Select the radio button next to the QoS policy that you want to edit or delete, and do one of the following:

- Click **Delete** to remove the QoS policy.
- Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.

3. Click **Apply** in the QoS Setup screen to save your changes.

USB Storage

5

Accessing and configuring a USB storage drive

This chapter describes how to access and configure a USB storage drive attached to your modem router. The USB port on the modem router can be used only to connect USB storage devices like flash drives or hard drives, or a printer. Do not connect computers, USB modems, CD drives, or DVD drives to the modem router USB port.

This chapter contains the following sections:

- *USB Drive Requirements*
- *ReadySHARE Access*
- *File-Sharing Scenarios*
- *Basic Settings*
- *USB Storage Advanced Settings*
- *Safely Remove a USB Drive*
- *Media Server Settings*
- *Specify Approved USB Devices*

For additional about ReadySHARE features, see *www.netgear.com/readyshare*.

USB Drive Requirements

The modem router works with 1.0 and 1.1 (USB Full Speed) and 2.0 (USB High Speed) standards. The approximate USB bus speeds are shown in the following table. Actual bus speeds can vary, depending on the CPU speed, memory, speed of the network, and other variables.

Table 3. USB Drive Speeds

Bus	Speed/Sec
USB 1.1	12 Mbits
USB 2.0	480 Mbits

The modem router works with most USB-compliant external flash and hard drives. For the most up-to-date list of USB drives that the modem router supports, go to:

http://kbserver.netgear.com/readyshare

The modem router supports both read and write for FAT16, FAT32, and NTFS.

Note: Some USB external hard drives and flash drives require you to load the drivers onto the computer before the computer can access the USB device. Such USB devices do not work with the modem router.

ReadySHARE Access

Once you have set up your modem router, you can connect any USB storage device and share the contents with others on your network.

You can access your USB device in any of the following ways:

- On Windows 7, Windows XP, Windows Vista, and Windows 2000 systems, select **Start > Run**, and enter **\\readyshare** in the dialog box. Click **OK**.
- On Windows 7, Windows XP, Windows Vista, and Windows 2000 systems, open Internet Explorer or Safari, and enter **\\readyshare** in the address bar.
- On Mac OSX (version 10.2 or later), enter **smb://readyshare** in the address bar.
- In My Network Places, enter **\\readyshare** in the address bar.

File-Sharing Scenarios

You can share files on the USB drive for a wide variety of business and recreational purposes. The files can be any PC, Mac, or Linux file type including text files, Word, PowerPoint, Excel, MP3, pictures, and multimedia. USB drive applications include:

- Sharing multimedia with friends and family such as MP3 files, pictures, and other multimedia with local and remote users.
- Sharing resources on your network. You can store files in a central location so that you do not have to power up a computer to perform local sharing. In addition, you can share files between Macintosh, Linux, and PC computers by using the USB drive as a go-between across the systems.
- Sharing files such as Word documents, PowerPoint presentations, and text files with remote users.

A few common uses are described in the following sections.

Sharing Photos

You can create your own central storage location for photos and multimedia. This method eliminates the need to log in to (and pay for) an external photo-sharing site.

➢ **To share files with your friends and family:**

1. Insert your USB drive into the USB port on the modem router either directly or with a USB cable.

    Computers on your local area network (LAN) can automatically access this USB drive using a web browser or Microsoft Networking.

2. If you want to specify read-only access or to allow access from the Internet, see *USB Storage Advanced Settings* on page 56.

Storing Files in a Central Location for Printing

This scenario is for a family that has one high-quality color printer directly attached to a computer, but not shared on the local area network (LAN). This family does not have a print server.

- One family member has photos on a Macintosh computer that she wants to print.
- The photo-capable color printer is directly attached to a PC, but not shared on the network.
- The Mac and PC are not visible to each other on the network.

➢ **To print photos from a Mac on the printer attached to a PC:**

1. On the Mac, access the USB drive by typing **\\readyshare** in the address field of a web browser. Then copy the photos to the USB drive.

2. On the PC, use a web browser or Microsoft Networking to copy the files from the USB drive to the PC. Then print the files.

Sharing Large Files over the Internet

Sending files that are larger than 5 MB can pose a problem for many email systems. The modem router allows you to share large files such as PowerPoint presentations or .zip files over the Internet. FTP can be used to download shared files from the modem router.

Sharing files with a remote colleague involves the following considerations:

- There are two user accounts: admin and guest. The password for admin is the same one that you use to access the modem router. By default, it is **password**. The guest user account has no password.

- On the FTP site, the person receiving the files uses the guest user account and enters the password. (FTP requires that you type something in the password field.)

- Be sure to select the **FTP (via Internet)** check box in the USB Storage Advanced Settings screen. This option supports both downloading and uploading of files.

Note: You can enable the HTTP (via Internet) option on the Advanced USB Storage screen to share large files. This option supports downloading files only.

Basic Settings

You can view or edit basic settings for the USB storage device attached to your modem router.

You can access this feature by selecting **Basic > ReadySHARE**, or **Advanced > USB Storage > ReadySHARE**.

The USB Storage (Basic Settings) screen displays:

USB Storage (Basic Settings)

⊙ Basic
○ ReadySHARE Printer

Network/Device Name \\readyshare

Available Network Folders

Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space

Edit

Safely Remove USB Device

Refresh

By default, the USB storage device is available to all computers on your local area network (LAN).

➢ **To access your USB device:**

1. Click the network device name or the share name in your computer's network folders list.

2. For SMB://readyshare, click **Connect**.

Note: If you logged in to the modem router before you connected your USB device, you might not see your USB device in the modem router screens. If this happens, log out and then log back in.

Add or Edit a Network Folder

1. You can access this feature by selecting **Basic > ReadySHARE**, and clicking **Edit**, or selecting **Advanced > USB Storage > Advanced Settings**.

2. Specify the changes that you want to make:

   • To add a folder, click **Create Network Folder**.

   • To edit a folder, select its radio button, and then click **Edit**.

3. can use this screen to select a folder, change the share name, or change the read access or write access from All – no password to .

The user name (account name) for All – no password is guest. The password for admin is the same one that is used to log in to the modem router. By default, it is password.

4. Click **Apply** for your changes to take effect.

USB Storage Advanced Settings

You can set up the device name, workgroups, and network folders for your USB device. On the Advanced tab, select **USB Storage > Advanced Settings** to display the following screen:

You can use this screen to specify access to the USB storage device.

*   **Network Device Name**. The default is readyshare. This is the name used to access the USB device connected to the modem router.

*   **Workgroup**. If you are using a Windows workgroup rather than a domain, the workgroup name is displayed here. The name works only in an operating system that supports NetBIOS, such as Microsoft Windows.

*   **Access Method**. The access methods are described here.

Network Connection. Enabled by default, this connection allows all users on the LAN to have access to the USB drive.

HTTP. Enabled by default. You can type **http://readyshare.routerlogin.net/shares** to access the USB drive.

HTTP (via Internet. Disabled by default. If you enable this setting, remote users can type **http://<*public IP address*/shares>** (for example, **http://1.1.10.102/shares**) or a URL

domain name to access the USB drive over the Internet. This setting supports file uploading only.

FTP. Disabled by default.

FTP (via Internet). Disabled by default. If you enable this setting, remote users can access the USB drive through FTP over the Internet. This setting supports both downloading and uploading of files.

Available Network Folders

You might need to scroll down to view this section of the screen:

- **Share Name**. If only 1 device is connected, the default share name is USB_Storage. You can click the name shown, or you can type it in the address field of your web Browser. If Not Shared is shown, the default share has been deleted, and no other share for the root folder exists. Click the link to change this setting.

- **Read/Write Access**. Shows the permissions and access controls on the network folder: All - no password (the default) allows all users to access the network folder. The password for admin is the same one that you use to log in to the modem router.

- **Folder Name**. Full path of the network folder.

- **Volume Name**. Volume name from the storage device (either USB drive or HDD).

- **Total/Free Space**. Shows the current utilization of the storage device.

Safely Remove a USB Drive

To remove a USB disk drive safely, select **USB Storage > Basic Settings**, and click the **Safely Remove USB Device** button. This takes the drive offline.

Media Server Settings

By default, the modem router is set up to act as a Ready DLNA Media server. This setting lets you view movies and photos on DLNA/UPnP AV–compliant media players, such as Xbox360, Playstation, and NETGEAR's Digital Entertainer Live.

To view these settings, select **Advanced > USB Storage > Media Server** to display the following screen:

By default the Enable Media Server check box and the Automatic (when new files are added) radio button are selected. When these options are selected, the modem router scans for media files whenever new files are added to the ReadySHARE USB hard drive.

Specify Approved USB Devices

For more security, you can set up the modem router to share approved USB devices only. You can access this feature from the Advanced Setup menu on the Advanced tab.

➢ **To set up approved USB devices:**

1. Select **Advanced > Advanced Setup > USB Settings. The following screen displays:**

2. **Click the Approved Devices** button. The USB Drive Approved Devices screen displays:

This screen shows the approved USB devices and the available USB devices. You can remove or add approved USB devices.

3. To add an approved USB device, select it from the Available USB Devices list, and then click **Add**.

4. Select the **Allow only approved devices** check box.

5. Click **Apply** so that your change takes effect.

If you want to work with another USB device, first click the **Safely Remove USB Device** button for the currently connected USB device. Connect the other USB device, and repeat this process.

Connect to the USB Drive from a Remote Computer

To connect to the USB drive from remote computers with a web browser, use the modem router's Internet port IP address. If you are using Dynamic DNS, you can type the DNS name, rather than the IP address. You can view the modem router's Internet IP address from the dashboard on the Basic Home screen or the Advanced Home screen.

Access the Modem Router's USB Drive Remotely Using FTP

➢ **To connect to the modem router's USB drive using a web browser:**

1. Connect to the modem router by typing **ftp://** and the Internet port IP address in the address field of Internet Explorer or Netscape Navigator, for example:

   ftp://10.1.65.4

   If you are using Dynamic DNS, you can type the DNS name, rather than the IP address.

2. Type the account name and password that has access rights to the USB drive. The user name (account name) for All – no password is **guest**.

3. The directories of the USB drive that your account has access to are displayed, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

Security

6

Keeping unwanted content out of your network

This chapter explains how to use the basic firewall features of the modem router to prevent objectionable content from reaching the computers and devices on your network.

This chapter includes the following sections:

- *Keyword Blocking of HTTP Traffic*
- *Firewall Rules to Control Network Access*
- *Port Triggering to Open Incoming Ports*
- *Port Forwarding to Permit External Host Communications*
- *How Port Forwarding Differs from Port Triggering*
- *Set Up Port Forwarding to Local Servers*
- *Set Up Port Triggering*
- *Schedule Blocking*
- *Security Event Email Notifications*

Keyword Blocking of HTTP Traffic

Use keyword blocking to prevent certain types of HTTP traffic from accessing your network. The blocking can be always or according to a schedule.

➢ **To set up keyword blocking:**

1. Select **Advanced > Security > Block Sites** to display the following screen:

2. Select one of the keyword blocking options:
   - **Per Schedule**. Turn on keyword blocking according to the Schedule screen settings.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.

3. In the Keyword field, enter a keyword or domain, click **Add Keyword,** and click **Apply**.

   The Keyword list supports up to 32 entries. Here are some sample entries:
   - Specify XXX to block http://www.badstuff.com/xxx.html.
   - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
   - Enter a period (**.**) to block all Internet browsing access.

➢ **To delete a keyword or domain:**

1. Select the keyword you want to delete from the list.
2. Click **Delete Keyword,** and then **Apply** to save your changes.

➢ **To specify a trusted computer:**

You can exempt one trusted computer from blocking and logging. The computer you exempt has to have a fixed IP address.

1. In the Trusted IP Address field, enter the IP address.
2. Click **Apply** to save your changes.

Firewall Rules to Control Network Access

Your modem router has a firewall that blocks unauthorized access to your wireless network and permits authorized inbound and outbound communications. Authorized communications are established according to inbound and outbound rules. The firewall has the following two default rules. You can create custom rules to further restrict the outbound communications or more widely open the inbound communications:

- **Inbound**. Block all access from outside except responses to requests from the LAN side.
- **Outbound**. Allow all access from the LAN side to the outside.

Set Up Firewall Rules

The Firewall Rules screen lets you add custom rules to make exceptions to the default rules. Exceptions can be based on the service or application, source or destination IP addresses, and time of day. You can log traffic that matches or does not match the rule and change the order of rule precedence.

All traffic attempting to pass through the firewall is subjected to the rules in the order shown in the Rules table from the top (highest precedence) to the default rules at the bottom. In some cases, the order of precedence is important to determine which communications are allowed into or out of the network.

➢ **To set up firewall rules:**

1. Select **Advanced > Security > Firewall Rules** to display the following screen:

2. To add an outbound rule, click **Add** under Outbound Services. To edit or delete a rule, select its button on the left side and click **Edit** or **Delete**.

3. To change the order of precedence:

   a. Select the button on the left side of the rule and click **Move**.

   b. At the prompt, enter the number of the new position and click **OK**.

4. To open or close instant messaging, select one of the following radio buttons:

   - **Close IM Ports**. Disables instant messaging traffic.
   - **Open IM Ports**. Enables instant messaging traffic. IM ports are open by default.

5. Click **Apply** to save your settings.

Port Triggering to Open Incoming Ports

Some application servers (such as FTP and IRC servers) send replies to multiple port numbers. Using the port triggering function of your router, you can tell the router to open additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the router, "When you initiate a session with destination port 6667, you have to also allow incoming traffic on port 113 to reach the originating computer." Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.

2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.

4. Noting your port triggering rule and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.

5. The IRC server sends a return message to your router using the NAT-assigned source port (for example, port 33333) as the destination port. The IRC server also sends an "identify" message to your router with destination port 113.

6. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.

7. Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is an active session for port 113, associated with your computer. The router replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.

8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or the relevant user groups or news groups.

Only one computer at a time can use the triggered application.

Port Forwarding to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer's browser needs to access a web server running on a computer in your local network. Using port forwarding, you can tell the router, "When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.1.123." The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your router. The remote computer composes a web page request message with the following destination information:

    Destination address. The IP address of www.example.com, which is the address of your router.

    Destination port number. 80, which is the standard port number for a web server process.

    The remote computer then sends this request message through the Internet to your router.

2. Your router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123. Therefore, your router modifies the destination information in the request message:

    The destination address is replaced with 192.168.1.123.

    Your router then sends this request message to your local network.

3. Your web server at 192.168.1.123 receives the request and composes a return message with the requested web page data. Your web server then sends this reply message to your router.

4. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the web page from www.example.com.

To configure port forwarding, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or the relevant user groups or news groups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

- Port triggering can be used by any computer on your network, although only one computer can use it at a time.

- Port forwarding is configured for a single computer on your network.

- With port triggering, the router does not need to know the computer's IP address in advance. The IP address is captured automatically.

- Port forwarding requires that you specify the computer's IP address during configuration, and the IP address can never change.

- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.

- Port forwarding is always active and does not need to be triggered.

Set Up Port Forwarding to Local Servers

The port forwarding feature lets you allow certain types of incoming traffic to reach servers on your local network. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

Use the Port Forwarding/Port Triggering screen to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded.

Before you start, determine which type of service, application, or game you want to provide, and the local IP address of the computer that will provide the service. The server computer has to always have the same IP address.

> **Tip:** To ensure that your server computer always has the same IP address, use the reserved IP address feature of your product. See *Address Reservation* on page 46.

➢ **To forward specific incoming protocols:**

1. Select **Advanced > Port Forwarding/Port Triggering** to display the following screen:

2. Leave the **Port Forwarding** radio button selected as the service type.

3. Click **Add,** and the following screen displays:

4. From the Service list, select the service or game that you will host on your network. If the service does not appear in the list, see *Add a Custom Service* on page 66.

5. In the Send to LAN Server field, enter the last digit of the IP address of your local computer that will provide this service.

6. Click **Apply**. The service appears in the list on the Port Forwarding screen.

Add a Custom Service

To define a service, game, or application that does not appear in the Service Name list, first determine which port number or range of numbers the application uses. You can usually determine this information by contacting the publisher of the application or user groups or news groups. When you have the port number information, follow these steps.

➢ **To add a custom service:**

1. Select **Advanced > Port Forwarding/Port Triggering**.

2. Select the **Port Forwarding** radio button as the service type.

3. Click the **Add Custom Service** button to display the following screen:

4. In the Service Name field, enter a descriptive name.

5. In the Protocol field, select the protocol. If you are unsure, select **TCP/UDP**.

6. In the Starting Port field, enter the beginning port number.

 • If the application uses a single port, enter the same port number in the Ending Port field.

 • If the application uses a range of ports, enter the ending port number of the range in the Ending Port field.

7. In the Server IP Address field, enter the IP address of your local computer that will provide this service.

8. Click **Apply**. The service appears in the list in the Port Forwarding/Port Triggering screen.

Edit or Delete a Port Forwarding Entry

➢ **To edit or delete a port forwarding entry:**

1. In the table, select the radio button next to the service name.

2. Click **Edit Service** or **Delete Service**.

Application Example: Make a Local Web Server Public

If you host a web server on your local network, you can use port forwarding to allow web requests from anyone on the Internet to reach your web server.

➢ **To make a local web server public:**

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation. In this example, your router always gives your web server an IP address of 192.168.1.33.

2. In the Port Forwarding/Port Triggering screen, configure the router to forward the HTTP service to the local address of your web server at **192.168.1.33**. HTTP (port 80) is the standard protocol for web servers.

3. (Optional) Register a host name with a Dynamic DNS service, and configure your router to use the name. To access your web server from the Internet, a remote user has to know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Set Up Port Triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

• More than one local computer needs port forwarding for the same application (but not simultaneously).

• An application needs to open incoming ports that are different from the outgoing port.

When port triggering is enabled, the router monitors outbound traffic looking for a specified outbound "trigger" port. When the router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The router then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

While port forwarding creates a static mapping of a port number or range to a single local computer, port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP).

To configure port triggering, you need to know which inbound ports the application needs, and the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or news groups.

➢ **To enable port triggering:**

1. Select **Advanced > Port Forwarding/Port Triggering** to display the Port Forwarding/Port Triggering screen.

2. Select the **Port Triggering** radio button to display the port triggering information.

3. Clear the **Disable Port Triggering** check box.

Note: If the Disable Port Triggering check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it is not used.

---
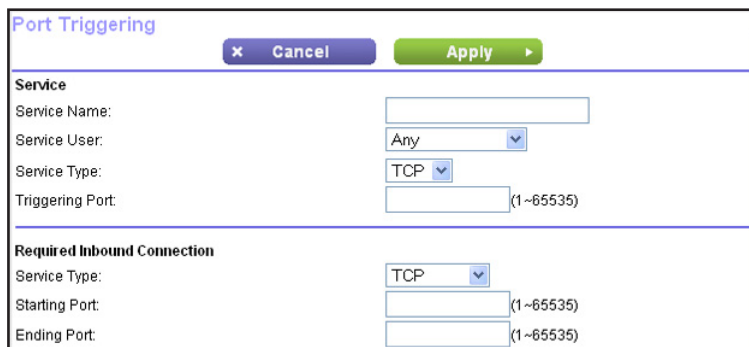
4. In the Port Triggering Timeout field, enter a value up to 9999 minutes. This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the router cannot be sure when the application has terminated.

➢ **To add a port triggering service:**

Make sure that you enable port triggering so that the service that you add will be used.

1. On the Port Triggering screen, click **Add Service**. The following screen displays:

2. In the Service Name field, type a descriptive service name.

3. In the Service User list, select Any (the default) to allow any computer on the Internet to use this service. Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.

4. Select the service type, either **TCP** or **UDP** or both (**TCP/UDP**). If you are not sure, select TCP/UDP.

5. In the Triggering Port field, enter the number of the outbound traffic port that will cause the inbound ports to be opened.

6. Enter the inbound connection port information in the Connection Type, Starting Port, and Ending Port fields.

7. Click **Apply**. The service appears in the Port Triggering Portmap Table.

Schedule Blocking

You can specify the days and time that you want to block Internet access.

➢ **To schedule blocking:**

1. Select **Advanced > Security > Schedule** to display the following screen:

2. Set up the schedule for blocking keywords and services.

   • **Days to Block**. Select days on which you want to apply blocking by selecting the appropriate check boxes, or select **Every Day** to select the check boxes for all days.

   • **Time of Day to Block**. Select a start and end time in 24-hour format, or select **All Day** for 24-hour blocking.

3. Select your time zone from the list. If you use daylight savings time, select the **Automatically adjust for daylight savings time** check box.

4. Click **Apply** to save your settings.

Security Event Email Notifications

To receive logs and alerts by email, provide your email information in the Email screen, and specify which alerts you want to receive and how often.

➢ **To set up email notifications:**

1. Select **Advanced > Security > Email** to display the following screen:

2. To receive email logs and alerts from the modem router, select the **Turn Email Notification On** check box.

3. In the Your Outgoing Mail Server field, enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration screen of your email program. If you leave this field blank, log and alert messages are not sent by email.

4. Enter the email address to which logs and alerts are sent in the Send to This Email Address field. This email address is also used for the From address. If you leave this field blank, log and alert messages are not sent by email.

5. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box. Fill in the User Name and Password fields for the outgoing email server.

6. You can have email alerts sent immediately when someone attempts to visit a blocked site, and you can specify that logs are sent automatically.

   If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is emailed to the specified email address. After the log is sent, the log is cleared from the modem router's memory. If the modem router cannot email the log file, the log buffer might fill up. In this case, the modem router overwrites the log and discards its contents.

7. Click **Apply** to save your settings.

Administration

7

Managing your network

This chapter describes the modem router settings for administering and maintaining your modem router and home network. See *Remote Management* on page 89 for information about upgrading or checking the status of your modem router over the Internet. See *Traffic Meter* on page 92 for information about monitoring Internet traffic.

This chapter includes the following sections:

- *Upgrade the Modem Router Firmware*
- *View Router Status*
- *View Logs of Web Access or Attempted Web Access*
- *Manage the Configuration File*
- *Set Password*

Upgrade the Modem Router Firmware

The modem router firmware (routing software) is stored in flash memory. You can update the firmware from the Administration menu on the Advanced tab. You might see a message at the top of the genie screens when new firmware is available for your product.

You can use the Check button on the Router Update screen to check and update to the latest firmware for your product if new firmware is available.

➢ **To check for new firmware and update your modem router:**

1. Select **Advanced > Administration > Router Upgrade** to display the following screen:

Click Check

2. Click **Check**.

The modem router finds new firmware information if any is available.

3. Click **Yes** to update and locate the firmware you downloaded (the file ends in .img).

⚠ **WARNING:**

When uploading firmware to the modem router, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

When the upload is complete, your modem router restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether or not you need to reconfigure the modem router after upgrading.

View Router Status

➢ **To view modem router status and usage information:**

Select **Advanced Home** or select **Administration > Router Status** to display the following screen:

Scroll to view more settings

Router Information

Hardware Version. The modem router model.

Firmware Version. The version of the modem router firmware. It changes if you upgrade the modem router firmware.

GUI Language Version. The localized language of the user interface.

LAN Port.

- **MAC Address**. The Media Access Control address. This is the unique physical address used by the Ethernet (LAN) port of the modem router.
- **IP Address**. The IP address used by the Ethernet (LAN) port of the modem router. The default is 192.168.1.1.
- **DHCP Server**. Identifies whether the modem router's built-in DHCP server is active for devices on the LAN.

Internet Port

MAC Address. The Media Access Control address, which is the unique physical address used by the Internet (WAN) port of the modem router.

IP Address. The IP address used by the Internet (WAN) port of the modem router. If no address is shown or the address is 0.0.0, the modem router cannot connect to the Internet.

Connection. This shows if the modem router is using a fixed IP address on the WAN. If the value is DHCP Client, the modem router obtains an IP address dynamically from the ISP.

IP Subnet Mask. The IP subnet mask used by the Internet (WAN) port of the modem router.

Domain Name Server. The Domain Name Server addresses used by the modem router. A Domain Name Server translates human-language URLs such as *www.netgear.com* into IP addresses.

Show Statistics Button

➢ **To view statistics:**

On the Router Status screen, in the Internet Provider (WAN) Setup pane, click **the Show Statistics** button to display the following screen:

System Up Time 00:11:36							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	PPPoE	1798	2564	0	378	11922	00:04:48
LAN1	Link down						
LAN2	100M/Full	17728	24410	0	35166	4143	00:10:08
LAN3	Link down						
LAN4	Link down						
WLAN b/g/n	145M	0	0	0	0	0	00:10:43
WLAN a/n							

ADSL Link	Downstream	Upstream
Link Rate	2977 Kbps	485 Kbps
Line Attenuation	34.0 dB	18.5 dB
Noise Margin	17.8 dB	16.0 dB

Poll Interval: 5 (secs) [Set Interval] [Stop]

The following information is displayed:

System Up Time. The time elapsed since the modem router was last restarted.

Port. The statistics for the WAN (Internet) and LAN (Ethernet) ports. For each port, the screen displays:

- **Status**. The link status of the port.
- **TxPkts**. The number of packets transmitted on this port since reset or manual clear.
- **RxPkts**. The number of packets received on this port since reset or manual clear.
- **Collisions**. The number of collisions on this port since reset or manual clear.
- **Tx B/s**. The current transmission (outbound) bandwidth used on the WAN and LAN ports.
- **Rx B/s**. The current reception (inbound) bandwidth used on the WAN and LAN ports.
- **Up Time**. The time elapsed since this port acquired the link.
- **Poll Interval**. The interval at which the statistics are updated in this screen.

To change the polling frequency, enter a time in seconds in the Poll Interval field and click **Set Interval**.

To stop the polling entirely, click **Stop**.

Administration

Connection Status Button

➢ **To view the Internet connection status:**

On the Router Status screen in the Internet Connection pane, click the **Connection Status** button to view connection status information.

The Release button returns the status of all items to 0. The Renew button refreshes the items. The Close Window button closes the Connection Status screen.

IP Address. The IP address that is assigned to the modem router.

Subnet Mask. The subnet mask that is assigned to the modem router.

Default Gateway. The IP address for the default gateway that the modem router communicates with.

DHCP Server. The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the modem router.

DNS Server. The IP address of the Domain Name Service server that provides translation of network names to IP addresses.

Lease Obtained. The date and time when the lease was obtained.

Lease Expires. The date and time that the lease expires.

Wireless Settings (2.4 GHz)

The following settings are displayed:

Name (SSID). The wireless network name (SSID) that the modem router uses.

Region. The geographic region where the modem router is being used. It might be illegal to use the wireless features of the modem router in some parts of the world.

Channel. The operating channel of the wireless port being used. The default channel is Auto. When Auto is selected, the modem router finds the best operating channel available. If you notice interference from nearby devices, you can select a different channel. Channels 1, 6, and 11 do not interfere with each other.

Mode. The wireless communication mode: Up to 54 Mbps, Up to 217 Mbps (default), and Up to 1300 Mbps.

Wireless AP. Indicates whether the radio feature of the modem router is enabled. If this feature is not enabled, the Wireless LED on the front panel is off.

Broadcast Name. Indicates whether the modem router is broadcasting its SSID.

Wireless Isolation. Wireless isolation prevents wireless clients from communicating with each other when they join the wireless network.

Wi-Fi Protected Setup. Indicates whether Wi-Fi Protected Setup is configured for this network.

View Logs of Web Access or Attempted Web Access

The log is a detailed record of the websites you have accessed or attempted to access. Up to 256 entries are stored in the log. Log entries appear only when keyword blocking is enabled and no log entries are made for the trusted user.

➢ **To view logs:**

Select **Advanced > Administration > Logs**. The Logs screen displays.
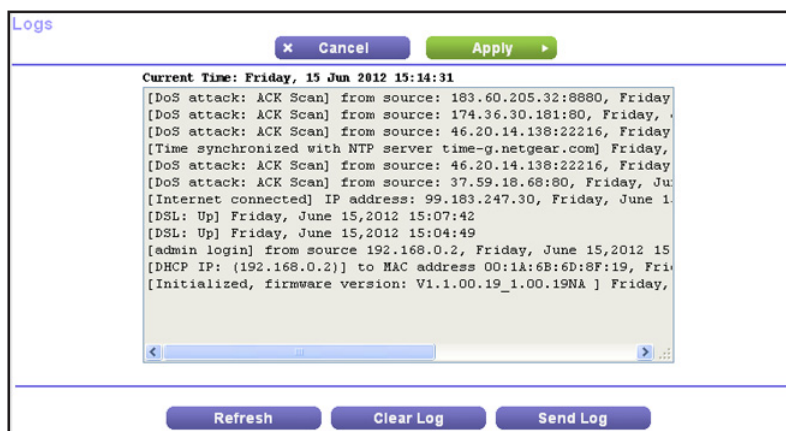
The log screen shows the following information:

- **Date and time**. The date and time the log entry was recorded.
- **Source IP**. The IP address of the initiating device for this log entry.
- **Target address**. The name or IP address of the website or news group visited or to which access was attempted.
- **Action**. Whether the access was blocked or allowed.

To refresh the log screen, click the **Refresh** button.

To clear the log entries, click the **Clear Log** button.

To email the log immediately, click the **Send Log** button.

Manage the Configuration File

The configuration settings of the modem router are stored within the modem router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

Back Up Settings

➢ **To back up the modem router's configuration settings:**

1. Select **Advanced > Administration > Backup Settings** to display the following screen:

Backup Settings

Save a copy of current settings

Backup Settings

Restore saved settings from a file

Browse…

Restore

Revert to factory default settings

✕ Erase

2. Click **Backup Settings** to save a copy of the current settings.
3. Choose a location to store the .cfg file that is on a computer on your network.

Restore Configuration Settings

➢ **To restore configuration settings that you backed up:**

1. Enter the full path to the file on your network or click the **Browse** button to find the file.
2. When you have located the .cfg file, click the **Restore** button to upload the file to the modem router.

Upon completion, the modem router reboots.

⚠ **WARNING:**

Do not interrupt the reboot process.

Erase

You can erase the configuration and restore the factory default settings. You might want to do this if you move the modem router to a different network or if you changed the password and have forgotten what it is (the default passwords are on the product label).

You can use the Restore Factory Settings button on the back of the modem router (see *Factory Settings* on page 134), or you can click the **Erase** button in this screen.

Erase sets the user name to admin, the password to password, and the LAN IP address to 192.168.1.1, and enables the modem router's DHCP.

Set Password

This feature let you change the default password that is used to log in to the modem router with the user name **admin**.

This is not the same as changing the password for wireless access. The label on the bottom of your modem router shows your unique wireless network name (SSID) and password for wireless access (see *Label* on page 8).

➢ **To set the password for the user name admin:**

1. Select **Advanced > Administration > Set Password** to display the following screen:

2. On the Set Password screen, type the old password, and type the new password twice.

3. If you want to be able to recover the password, select the **Enable Password Recovery** check box.

4. Click **Apply** so that your changes take effect.

Password Recovery

NETGEAR recommends that you enable password recovery if you change the password for the router's user name of admin. Then you will have an easy way to recover the password if it is forgotten. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

➢ **To set up password recovery:**

1. Select the **Enable Password Recovery** check box.

2. Select two security questions, and provide answers to them.

3. Click **Apply** to save your changes.

When you use your browser to access the router, the login window displays. If password recovery is enabled, when you click Cancel, the password recovery process starts. You can then enter the saved answers to the security questions to recover the password.

Advanced Settings

8

This chapter describes the advanced features of your modem router. The information is for readers with advanced networking knowledge who want to set the modem router up for unique situations such as when remote access from the Internet by IP or domain name is needed.

> **Note:** The Port Forwarding/Port Triggering screen can be accessed both through the Advanced Setup menu and through the Firewall Rules screen. For information about port forwarding and port triggering, see *Chapter 6, Security*.

This chapter includes the following sections:

- *Advanced Wireless Settings*
- *Wireless Repeating Function (WDS)*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *USB Settings*
- *Universal Plug and Play*
- *IPv6*
- *Traffic Meter*
- *Change the Device Mode*

Advanced Wireless Settings

➢ **To go to the Advanced Wireless Settings screen:**

Select **Advanced > Advanced Setup > Wireless Settings** to display the following screen:

The following settings are available in this screen:

Enable Wireless Router Radio. You can completely turn off the wireless portion of the wireless modem router by clearing this check box. Select this check box again to enable the wireless portion of the modem router. When the wireless radio is disabled, other members of your household can use the modem router by connecting their computers to the modem router with an Ethernet cable.

Note: The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.

Turn off wireless signal by schedule. You can use this feature to turn off the wireless signal from your modem router at times when you do not need a wireless connection. For instance, you could turn it off for the weekend if you leave town.

WPS Settings.You can add WPS devices to your network.

Wireless Card Access List. You can restrict access to your network to specific devices based on their MAC address. See *Restrict Wireless Access by MAC Address* on page 82.

Restrict Wireless Access by MAC Address

You can set up a list of computers and wireless devices that are allowed to join the wireless network. This list is based on the unique MAC address of each computer and device.

Each network device has a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of the wireless card or network interface device. If you do not have access to the label, you can display the MAC address using the network configuration utilities of the computer. You might also find the MAC addresses in the Attached Devices screen.

➢ **To restrict access based on MAC addresses:**

1. Select **Advanced > Advanced Setup > Wireless Settings** and click the **Setup Access List** to display the Wireless Card Access List.

2. Click **Add** to add a wireless device to the wireless access control list.

   The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses.

3. If the computer or device you want is in the Available Wireless Cards list, select that radio button; otherwise, type a name and the MAC address. You can usually find the MAC address on the bottom of the wireless device.

   Tip: You can copy and paste the MAC addresses from the Attached Devices screen into the MAC Address field of this screen. To do this, use each wireless computer to join the wireless network. The computer should then appear in the Attached Devices screen.

4. Click **Add** to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen.

5. Add each computer or device you want to allow to connect wirelessly.

6. Select the **Turn Access Control On** check box.

7. Click **Apply**.

Wireless Repeating Function (WDS)

You can set the N300 Wireless ADSL2+ Modem Router up to be used as a wireless access point (AP). Doing this enables the modem router to act as a wireless repeater. A wireless repeater connects to another wireless modem router as a client where the network to which it connects becomes the ISP service.

Wireless repeating is a type of Wireless Distribution System (WDS). A WDS allows a wireless network to be expanded through multiple access points instead of using a wired backbone to link them. The following figure shows a wireless repeating scenario.

Base station
access point

Repeater
access point
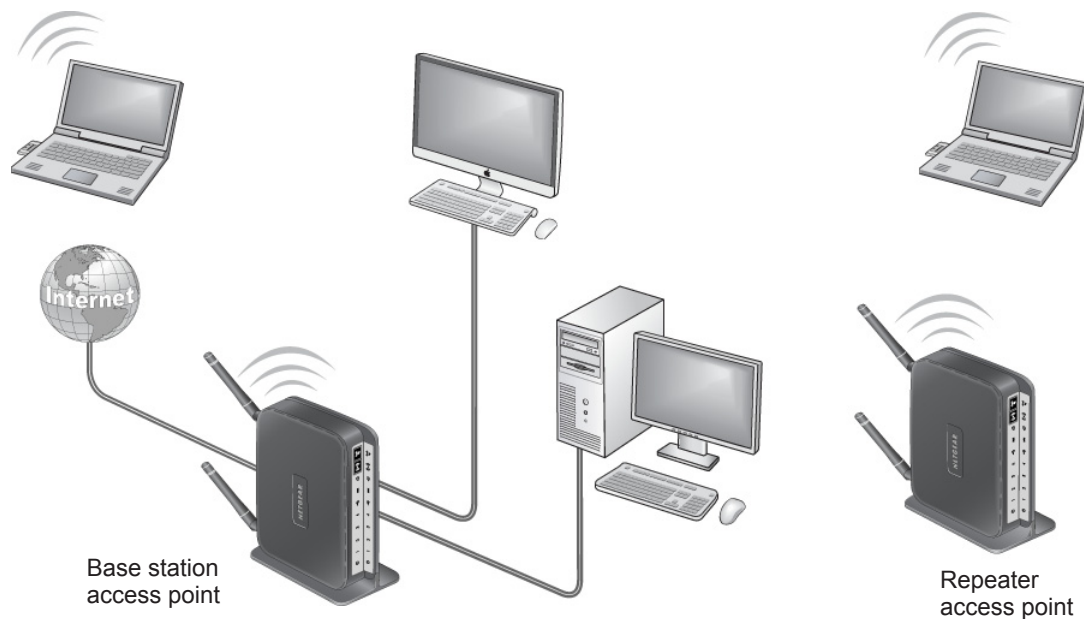
Figure 8. Wireless repeating scenario

Note: If you use the wireless repeating function, you need to select either WEP or None as a security option in the Wireless Settings screen. The WEP option displays only if you select the wireless mode Up to 54 Mbps in the Wireless Settings screen.

Wireless Base Station. The modem router acts as the parent access point, that bridges traffic to and from the child repeater access point. The base station also handles wireless and wired local computers. To configure this mode, you have to know the MAC addresses of the child repeater access point. Often, the MAC address is on the product label.

Wireless Repeater. The modem router sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you have to know the MAC address of the remote parent access point.

The DGN2200v3 modem router is always in dual band concurrent mode, unless you turn off one radio.If you enable the wireless repeater in either radio band, the wireless base station or wireless repeater cannot be enabled in the other radio band. However, if you enable the wireless base station in either radio band and use the other radio band as a wireless modem router or wireless base station, dual band concurrent mode is not affected.

To set up a wireless network with WDS, both access points have to meet the following conditions:

- Both access points have to use the same SSID, wireless channel, and encryption mode.
- Both access points have to be on the same LAN IP subnet. That is, all of the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) are configured to operate in the same LAN network address range as the access points.

Wireless Repeating Function

➢ **To view or change the wireless repeater settings for the modem router:**

Select **Advanced > Advanced Setup > Wireless Repeating**.

- **Enable Wireless Repeating Function (2.4 GHz b/g/n)**. Select this check box to use the wireless repeating function.

  Disable Wireless Client Association. If your modem router is the repeater, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

  - If you are setting up a point-to-point bridge, select this check box.
  - If you want all client traffic to go through the other access point (repeater with wireless client association), leave this check box cleared.

- If you want all client traffic to go through the other access point (repeater with wireless client association), leave this check box cleared.

- **Wireless Repeater**. If your modem router is the repeater, select this radio button.

Repeater IP Address. If your modem router is the repeater, enter the IP address of the other access point.

Base Station MAC Address. If your modem router is the repeater, enter the MAC address for the access point that is the base station.

• **Wireless Base Station**. If your modem router is the base station, select this check box.

Repeater MAC Address (1 through 4). If your modem router is the base station, it can act as the "parent" of up to 4 other access points. Enter the MAC addresses of the other access points in these fields.

Set Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You have to know the wireless settings for both units. You have to know the MAC address of the remote unit. First, set up the base station, and then set up the repeater.

➢ **To set up the base station:**

1. Set up both units with exactly the same wireless settings (SSID, mode, channel, and security). The wireless security option has to be set to None or WEP.

2. Select **Advanced > Advanced Setup > Wireless Repeating Function** to display the Wireless Repeating Function screen.

3. In the Wireless Repeating Function screen.

4. Select the **Enable Wireless Repeating Function** check box and select the **Wireless Base Station** radio button.

5. Enter the MAC address for one or more repeater units.

6. Click **Apply** to save your changes.

Set Up a Repeater Unit

Use a wired Ethernet connection to set up the repeater unit to avoid conflicts with the wireless connection to the base station.

Note: If you are using the DGN2200v3 base station with a different router product NETGEARas the repeater, you might need to change additional configuration settings. In particular, you should disable the DHCP server function on the wireless repeater AP.

➢ **To configure the modem router as a repeater unit:**

1. Log in to the modem router that will be the repeater. Select **Basic > Wireless Settings** and verify that the wireless settings match the base unit exactly. The wireless security option has to be set to **WEP** or **None**.

2. Select **Advanced > Wireless Repeating Function**.

3. Select the **Enable Wireless Repeating Function check box.**

4. **Select** the **Wireless Repeater** radio button.

5. Fill in the Repeater IP Address field. This IP address has to be in the same subnet as the base station, but different from the LAN IP address of the base station.

6. Click **Apply** to save your changes.

7. Verify connectivity across the LANs.

   A computer on any wireless or wired LAN segment of the modem router should be able to connect to the Internet or share files and printers with any other wireless or wired computer or server connected to the other access point.

Dynamic DNS

If your Internet service provider (ISP) gave you a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. This type of service lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service does not work because private addresses are not routed on the Internet.

Your modem router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. First visit their website at *http://www.dyndns.org* and obtain an account and host name that you configure in the modem router. Then, whenever your ISP-assigned IP address changes, your modem router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your modem router at *http://hostname.dyndns.org*.

➢ **To set up Dynamic DNS:**

1. Select **Advanced > Advanced Setup > Dynamic DNS** to display the following screen:

2. Register for an account with one of the Dynamic DNS service providers whose names appear in the Service Provider list. For example, for DynDNS.org, select *www.dyndns.org*.

3. Select the **Use a Dynamic DNS Service** check box.

4. Select the name of your Dynamic DNS service provider.

5. Type the host name (or domain name) that your Dynamic DNS service provider gave you.

6. Type the user name for your Dynamic DNS account. This is the name that you use to log in to your account, not your host name.

7. Type the password (or key) for your Dynamic DNS account.

8. If your Dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use Wildcards** check box to activate this feature.

   For example, the wildcard feature causes **.yourhost.dyndns.org* to be aliased to the same IP address as yourhost.dyndns.org.

9. Click **Apply** to save your configuration.

Static Routes

Static routes provide additional routing information to your modem router. Typically, you do not need to add static routes. You have to configure static routes only for unusual cases such as multiple modem routers or multiple IP subnets on your network.

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.

- You have an ISDN modem router on your home network for connecting to the company where you are employed. This modem router's address on your LAN is 192.168.1.100.

- Your company's network address is 134.177.0.0.

When you first configured your modem router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your modem router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you have to define a static route, telling your modem router that 134.177.0.0 should be accessed through the ISDN modem router at 192.168.1.100. In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.

- The Gateway IP Address field specifies that all traffic for these addresses should be forwarded to the ISDN modem router at 192.168.1.100.

- A metric value of 1 will work since the ISDN modem router is on the LAN.

- Private is selected only as a precautionary security measure in case RIP is activated.

➢ **To set up a static route:**

1. Select **Advanced > Advanced Setup > Static Routes**.

2. Click **Add** to display the following screen:

3. In the Route Name field, type a name for this static route (for identification purposes only.)

4. Select the **Private** check box if you want to limit access to the LAN only. If Private is selected, the static route is not reported in RIP.

5. Select the **Active** check box to make this route effective.

6. Type the destination IP address of the final destination.

7. Type the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.

8. Type the gateway IP address, which has to be a modem router on the same LAN segment as the N300 Wireless ADSL2+ Modem Router.

9. Type a number from 1 through 15 as the metric value.

    This value represents the number of modem routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.

10. Click **Apply** to add the static route.

Remote Management

The remote management feature lets you upgrade or check the status of your N300 Wireless ADSL2+ Modem Router over the Internet.

➢ **To set up remote management:**

1. Select **Advanced > Advanced Setup > Remote Management**.

> **Note:** *Be sure to change the modem router's default login password to a secure password. The ideal password contains no dictionary words from any language and contains upper-case and lower-case letters, numbers, and symbols. It can be up to 30 characters.*

2. Select the **Turn Remote Management On** check box.

3. Under Allow Remote Access By, specify the external IP addresses to be allowed to access the modem router's remote management.

> **Note:** *For enhanced security, restrict access to as few external IP addresses as practical.*

- To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.

- To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address to define the allowed range.

- To specify IP addresses, select **IP Address List** and type in the allowed IP addresses.

- To allow access from any IP address on the Internet, select **Everyone**.

4. Specify the port number for accessing the management interface.

    Normal web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote web management interface. Choose a number from 1024 to 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

5. Click **Apply** so that your changes take effect.

6. When you access your modem router from the Internet, type your modem router's WAN IP address into your browser's address or location field followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter **http://134.177.0.123:8080** in your browser.

USB Settings

For added security, the modem router can be set up to share only approved USB devices. See *Specify Approved USB Devices* on page 58 for the procedure.

Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance (a feature in Windows XP), you should enable UPnP.

➢ **To turn on Universal Plug and Play:**

Select **Advanced > Advanced Setup > UPnP**. The UPnP screen displays.

The available settings and information in this screen are:

Turn UPnP On. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If this check box is not selected, the modem router does not allow any device to automatically control the resources, such as port forwarding (mapping) of the modem router.

Advertisement Period. The advertisement period is how often the modem router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations can compromise the freshness of the device status, but can significantly reduce network traffic.

Advertisement Time to Live. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which is fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it might be necessary to increase this value.

UPnP Portmap Table. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the modem router and which ports (internal and external) that device has opened. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

7. Click **Apply** to save your settings.

IPv6

You can use this feature to set up an IPv6 Internet connection type if genie does not detect it automatically.

➢ **To set up an IPv6 Internet connection type:**

1. Select **Advanced > Advanced Setup > IPv6** to display the following screen:

2. Select the IPv6 connection type from the list. Your Internet service provider (ISP) can provide this information.
   - If your ISP did not provide details, you can select **IPv6 Tunnel**.
   - If you are not sure, select **Auto Detect** so that the modem router detects the IPv6 type that is in use.
   - If your Internet connection does not use PPPoE, DHCP, or fixed, but is IPv6, then select **IPv6 auto config**.

3. Click **Apply** so that your changes take effect.

Traffic Meter

Traffic metering allows you to monitor the volume of Internet traffic that passes through your modem router's Internet port. With the Traffic Meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

➢ **To monitor Internet traffic:**

1. Click **Advanced > Advanced Setup > Traffic Meter** to display the following screen:

Scroll to view
more settings

2. To enable the Traffic Meter, select the **Enable Traffic Meter** check box.

3. If you want to record and restrict the volume of Internet traffic, select the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:

   No Limit. No restriction is applied when the traffic limit is reached.

   Download only. The restriction is applied to incoming traffic only.

   Both Directions. The restriction is applied to both incoming and outgoing traffic.

4. You can limit the amount of data traffic allowed per month by specifying how many Mbytes per month are allowed or by specifying how many hours of traffic are allowed.

5. Set the Traffic Counter to begin at a specific time and date.

6. Set up Traffic Control to issue a warning message before the monthly limit of Mbytes or hours is reached. You can select one of the following to occur when the limit is attained:
   • The Internet LED flashes green or amber.
   • The Internet connection is disconnected and disabled.

7. Set up Internet Traffic Statistics to monitor the data traffic.

8. Click the **Traffic Status** button to get a live update on Internet traffic status.
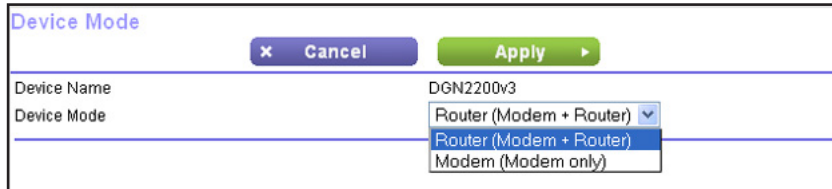
9. Click **Apply** to save your settings.

Change the Device Mode

The modem includes a built-in router. If you want to configure the modem as a "pure bridge" in Modem mode, first set up the Internet connection and then change the Device Mode setting to Modem mode. In Modem mode, the device acts as a "pure bridge" or DSL modem. When the device is in Modem mode, features that are not available are grayed out.

➢ **To change the device mode:**

1. Select **Advanced > Device Mode**. The following screen displays:

    By default, the modem is in Router mode.

2. Select the device mode that you want from the drop-down list.
3. Click **Apply** so that your changes take effect.

Virtual Private Networking

9

This chapter describes how to use the virtual private networking (VPN) features of the modem router. VPN communications paths are called tunnels. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer. See *Appendix B, VPN Configuration* to learn more about VPNs.

This chapter is organized as follows:

Overview of VPN Configuration

Two common scenarios for VPN tunnels are between a remote PC and a network gateway; and between two or more network gateways. The DGN2200v3 supports both types. The DGN2200v3 supports up to five concurrent tunnels.

Client-to-Gateway VPN Tunnels

Client-to-gateway VPN tunnels provide secure access from a remote PC, such as a telecommuter connecting to an office network.
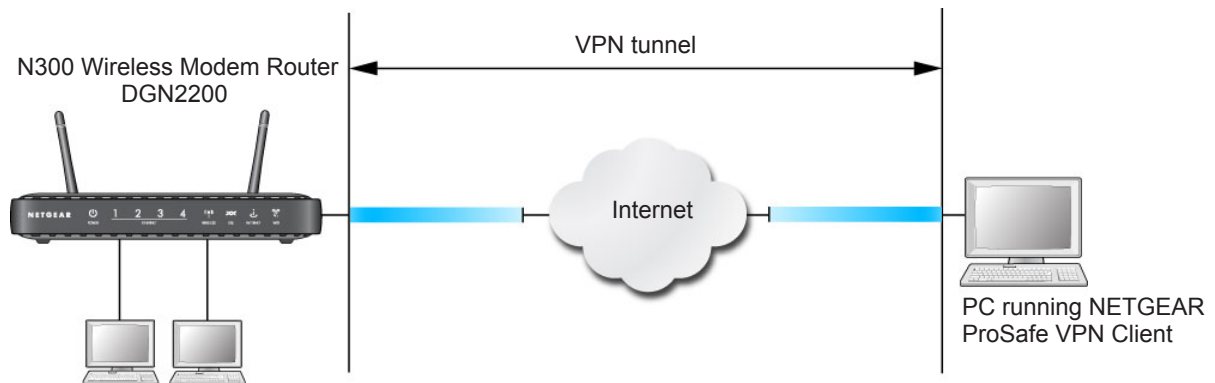

Figure 9. Telecommuter VPN tunnel

A VPN client access allows a remote PC to connect to your network from any location on the Internet. The remote PC is one tunnel endpoint, running the VPN client software. The modem router on your network is the other tunnel endpoint. (See *Set Up a Client-to-Gateway VPN Configuration* on page 98.)

Gateway-to-Gateway VPN Tunnels

Gateway-to-gateway VPN tunnels provide secure access between networks, such as a branch or home office and a main office.
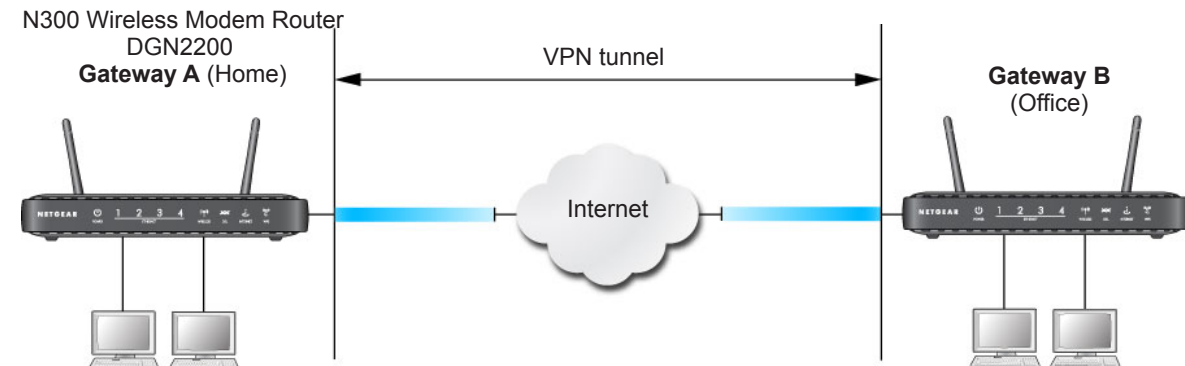

Figure 10. VPN tunnel between networks

A VPN between two or more NETGEAR VPN-enabled routers is a good way to connect branch or home offices and business partners over the Internet. VPN tunnels also enable access to network resources across the Internet. In this case, use gateways on each end of the tunnel to form the VPN tunnel end points. See *Set Up a Gateway-to-Gateway VPN Configuration* on page 108 for information about how to set up this configuration.

Plan a VPN

When you set up a VPN, it is helpful to plan the network configuration and record the configuration parameters on a worksheet:

Table 4. VPN Tunnel Configuration Worksheet

Parameter		Value to Be Entered	Field Selection	
Connection Name			N/A	
Pre-Shared Key			N/A	
Secure Association		N/A	Main Mode	Manual Keys
Perfect Forward secrecy		N/A	Enabled	Disabled
Encryption Protocol		N/A	DES	3DES
Authentication Protocol		N/A	MD5	SHA-1
Diffie-Hellman (DH) Group		N/A	Group 1	Group 2
Key Life in seconds			N/A	
IKE Life Time in seconds			N/A	
VPN Endpoint	**Local IPSecID**	**LAN IP Address**	**Subnet Mask**	**FQDN or Gateway IP (WAN IP Address**

To set up a VPN connection, you need to configure each endpoint with specific identification and connection information describing the other endpoint. You configure the outbound VPN settings on one end to match the inbound VPN settings on other end, and vice versa.

This set of configuration information defines a security association (SA) between the two VPN endpoints. When planning your VPN, you have to make a few choices first:

•   Will the local end be any device on the LAN, a portion of the local network (as defined by a subnet or by a range of IP addresses), or a single PC?

•   Will the remote end be any device on the remote LAN, a portion of the remote network (as defined by a subnet or by a range of IP addresses), or a single PC?

- Will either endpoint use fully qualified domain names (FQDNs)? FQDNs supplied by Dynamic DNS providers (see *Using a Fully Qualified Domain Name (FQDN)* on page 141) can allow a VPN endpoint with a dynamic IP address to initiate or respond to a tunnel request. Otherwise, the side using a dynamic IP address has to always be the initiator.
- Which method will you use to configure your VPN tunnels?
    - The VPN Wizard using VPNC defaults (see *Table 5, Parameters Recommended by the VPNC and Used in the VPN Wizard* on page 97).
    - The typical automated Internet Key Exchange (IKE) setup (see *Use Auto Policy to Configure VPN Tunnels* on page 116).
    - A manual keying setup in which you need to specify each phase of the connection (see *Use Manual Policy to Configure VPN Tunnels* on page 123)?

Table 5. Parameters Recommended by the VPNC and Used in the VPN Wizard

Parameter	Factory Default Setting
Secure Association	Main Mode
Authentication Method	Pre-Shared Key
Encryption Method	3DES
Authentication Protocol	SHA-1
Diffie-Hellman (DH) Group	Group 2 (1024 bit)
Key Life	8 hours
IKE Life Time	1 hour

- What level of IPSec VPN encryption will you use?
    - **DES**. The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56-bit key. Faster but less secure than 3DES.
    - **3DES**. Triple DES achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
- What level of authentication will you use?
    - **MD5**. 128 bits, faster but less secure.
    - **SHA-1**. 160 bits, slower but more secure.

VPN Tunnel Configuration

There are two tunnel configurations and three ways to configure them:

- Use the VPN Wizard to configure a VPN tunnel (recommended for most situations):
    - See *Set Up a Client-to-Gateway VPN Configuration* on page 98.
    - See *Set Up a Gateway-to-Gateway VPN Configuration* on page 108.

- See *Use Auto Policy to Configure VPN Tunnels* on page 116 when the VPN Wizard and its VPNC defaults are not appropriate for your special circumstances, but you want to automate the Internet Key Exchange (IKE) setup.

- See *Use Manual Policy to Configure VPN Tunnels* on page 123 when the VPN Wizard and its VPNC defaults are not appropriate for your special circumstances and you have to specify each phase of the connection. You manually enter all the authentication and key parameters. You have more control over the process; however, the process is more complex, and there are more opportunities for errors or configuration mismatches between your DGN2200v3 and the corresponding VPN endpoint gateway or client workstation.

> **Note:** NETGEAR publishes additional interoperability scenarios with various gateway and client software products. Look on the NETGEAR website at *www.netgear.com* for these interoperability scenarios.

Set Up a Client-to-Gateway VPN Configuration

Setting up a VPN between a remote PC running the NETGEAR ProSafe VPN Client and a network gateway involves these two steps:

- *Step 1: Configure the Gateway-to-Client VPN Tunnel* on page 98 describes how to use the VPN Wizard to configure the VPN tunnel between the remote PC and network gateway.

- *Step 2: Configure the NETGEAR ProSafe VPN Client* on page 101 shows how to configure the NETGEAR ProSafe VPN Client endpoint.
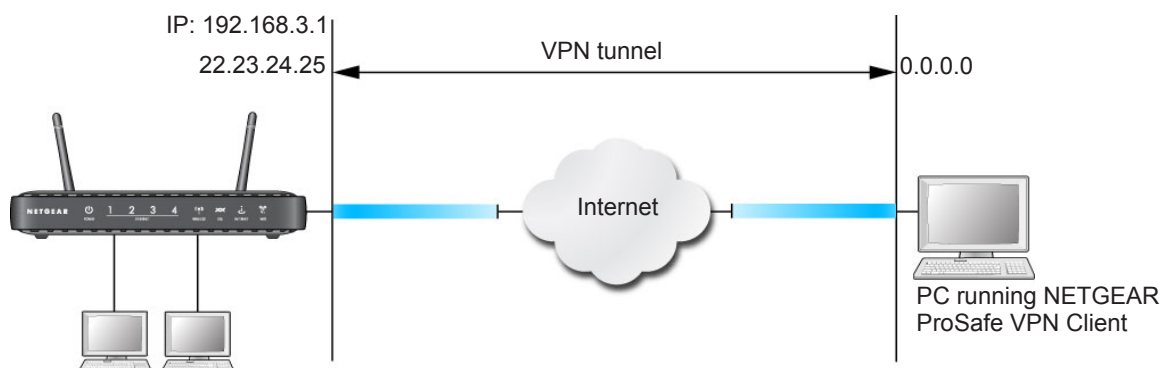

Figure 11. Client-to-gateway VPN tunnel

Step 1: Configure the Gateway-to-Client VPN Tunnel

This section describes using the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in *Table 5* on page 97. If you have special requirements not

covered by these VPNC-recommended parameters, see *Set Up VPN Tunnels in Special Circumstances* on page 116 for information about how to set up the VPN tunnel.

The following worksheet identifies the parameters used in this procedure, which are highlighted in blue. For a blank worksheet, see *Plan a VPN* on page 96.

Table 6. VPN Tunnel Configuration Worksheet

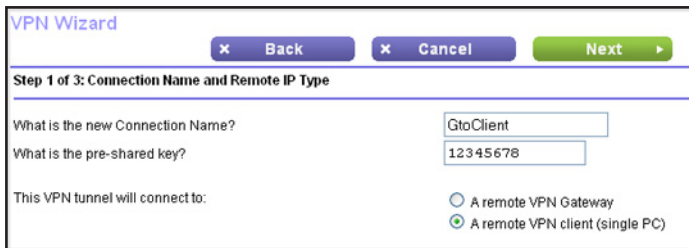| Parameter		Value to Be Entered	Field Selection	
Connection Name		RoadWarrior	N/A	
Pre-Shared Key		12345678	N/A	
Secure Association		N/A	Main Mode	Manual Keys
Perfect Forward secrecy		N/A	Enabled	Disabled
Encryption Protocol		N/A	DES	3DES
Authentication Protocol		N/A	MD5	SHA-1
Diffie-Hellman (DH) Group		N/A	Group 1	Group 2
Key Life in seconds		28800 (8 hours)	N/A	
IKE Life Time in seconds		3600 (1 hour)	N/A	
VPN Endpoint	**Local IPSecID**	**LAN IP Address**	**Subnet Mask**	**FQDN or Gateway IP (WAN IP Address)**
Client	toGateway	N/A	N/A	Dynamic
Gateway	toClient	192.168.3.1	255.255.255.0	22.23.24.25

➢ **To configure a client-to-gateway VPN tunnel using the VPN Wizard:**

1. Select **Advanced > Advanced - VPN > VPN Wizard**.
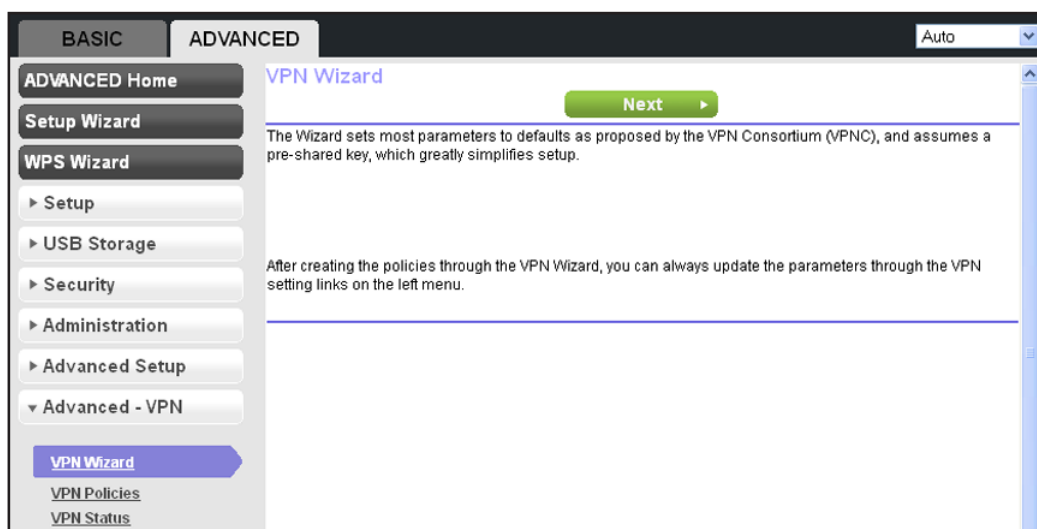
2. Click **Next**.

3. Fill in the Connection Name and pre-shared key fields.

The connection name is for convenience and does not affect how the VPN tunnel functions.
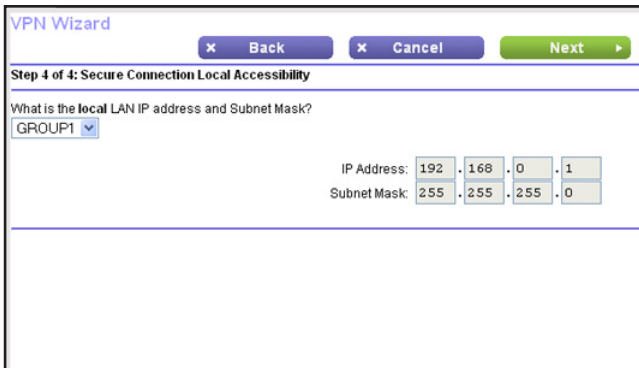
4. Select the radio button for **A remote VPN client (single PC)**, and click **Next**.

5. Enter the remote IP address and subnet mask, and click **Next**.

The Summary screen displays:

Note: *To view the VPNC-recommended authentication and encryption settings used by the VPN Wizard, click the **here** link.*

6. Click **Done**. The VPN Policies screen displays, showing that the new tunnel is enabled:

VPN Policies							
		✕ Back	✕ Cancel	Apply ▶			
Policy Table							
	#	Enable	Name	Type	Local	Remote	ESP
◉	1	☑	GtoClient	Auto	192.168.0.1 / 255.255.255.0	---	3DES
			✏ Edit		✕ Delete		
		+ Add Auto Policy		+ Add Manual Policy			

To view or modify the tunnel settings, select its radio button and click **Edit**.

See *Use Auto Policy to Configure VPN Tunnels* on page 116 for information about how to enable the IKE keep-alive capability on an existing VPN tunnel.

Step 2: Configure the NETGEAR ProSafe VPN Client

This section describes how to configure the NETGEAR ProSafe VPN Client on a remote PC. These instructions assume that the PC running the client has a dynamically assigned IP address.

The PC has to have the NETGEAR ProSafe VPN Client program installed that supports IPSec. Go to the NETGEAR website (*http://www.netgear.com*) for information about how to purchase the NETGEAR ProSafe VPN Client.

Note: Before installing the NETGEAR ProSafe VPN Client software, be sure to turn off any virus protection or firewall software you might be running on your PC. You might need to insert your Windows CD to complete the installation.

---

1. Install the NETGEAR ProSafe VPN Client on the remote PC, and then reboot.
   a. Install the IPSec component. You might have the option to install either the VPN adapter or the IPSec component or both. The VPN adapter is not necessary.

   If you do not have a modem or dial-up adapter installed in your PC, you might see the warning message stating "The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed." You can disregard this message.

   b. Reboot the remote PC.

   The ProSafe icon (🔲) is in the system tray.

   c. Double-click the ProSafe icon to open the Security Policy Editor.

2. Add a new connection.
   a. Run the NETGEAR ProSafe Security Policy Editor program, and, using the *Table 6* on page 99, create a VPN connection.

---

b. From the Edit menu of the Security Policy Editor, select **Add**, and then click **Connection**.
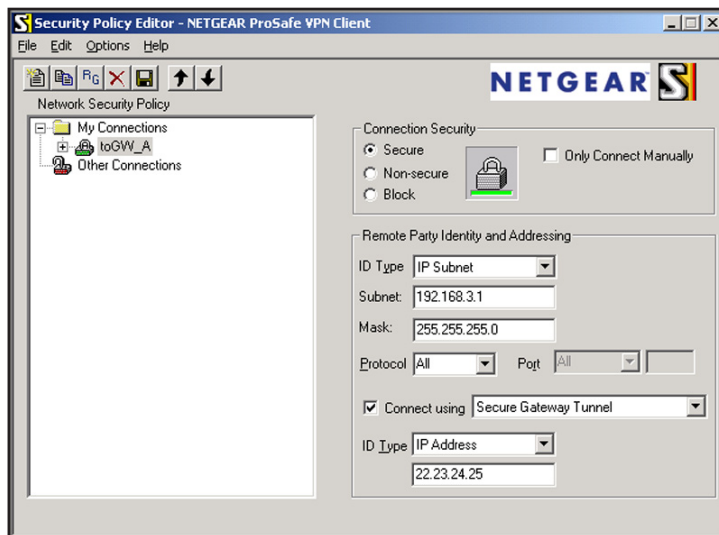
A New Connection listing appears in the list of policies.

c. Rename the new connection so that it matches the Connection Name field in the VPN Settings screen of the modem router on LAN A. Choose connection names that make sense to the people using and administering the VPN.


Note: In this example, the connection name used on the client side of the VPN tunnel is toGW_A, and it does not have to match the RoadWarrior connection name used on the gateway side of the VPN tunnel because connection names are irrelevant to how the VPN tunnel functions.

---

d. Enter the following settings:
   - Connection Security: **Secure**.
   - ID Type: **IP Subnet**.
   - Subnet.: In this example, type **192.168.3.1** as the network address of the modem router.
   - Mask: Enter **255.255.255.0** as the LAN subnet mask of the modem router.
   - Protocol: Select **All** to allow all traffic through the VPN tunnel.

e. Select **Connect using** and then select the **Secure Gateway Tunnel** check box.

f. In the ID Type drop-down list, select **IP Address**.

g. I the field directly below the ID Type drop-down list, enter the public WAN IP address of the modem router. In this example, 22.23.24.25 is used.

The resulting connection settings are shown in *Figure c* on page 103.

3. Configure the security policy in the NETGEAR ProSafe VPN Client software:

   a. In the Network Security Policy list, expand the new connection by double-clicking its name or clicking the + symbol. My Identity and Security Policy subheadings appear below the connection name.

   b. Click the **Security Policy** subheading to view the Security Policy settings.
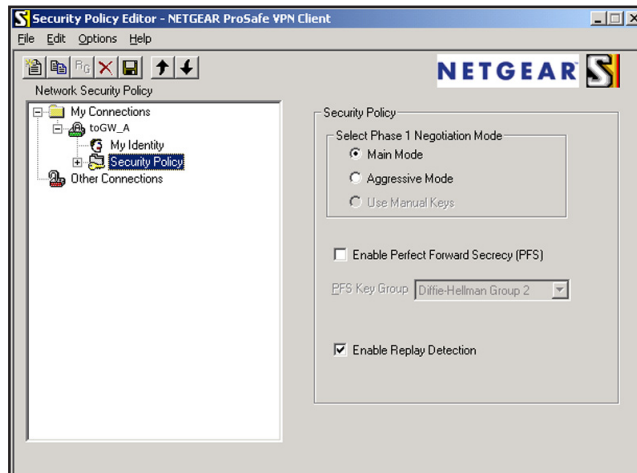
Security Policy settings, Client-to-Gateway A

   c. In the Select Phase 1 Negotiation Mode section of the screen, select the **Main Mode** radio button.

4. Configure the VPN client identity.

   In this step, you provide information about the remote VPN client PC. You need to provide the pre-shared key that you configured in the modem router and either a fixed IP address or a fixed virtual IP address of the VPN client PC.

   a. In the Network Security Policy list on the left side of the Security Policy Editor window, click **My Identity**.
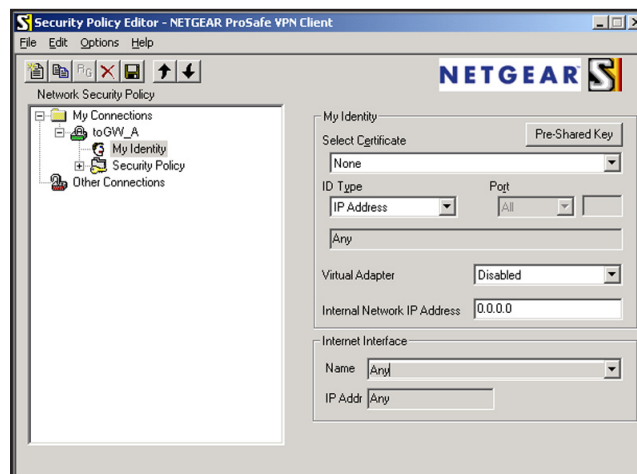
   b. In the Select Certificate drop-down list, select **None**.

   c. In the ID Type drop-down list, select **IP Address**. If you are using a virtual fixed IP address, enter this address in the Internal Network IP Address field. Otherwise, leave this field empty.

d. In the Internet Interface section of the screen, select the adapter that you use to access the Internet. If you have a dial-up Internet account, select **PPP Adapter** in the Name field. If you have a dedicated cable or DSL line, select your Ethernet adapter. If you will be switching between adapters or if you have only one adapter, select **Any**.

**e.** In the My Identity section of the screen, click the **Pre-Shared Key** button. The Pre-Shared Key screen displays:
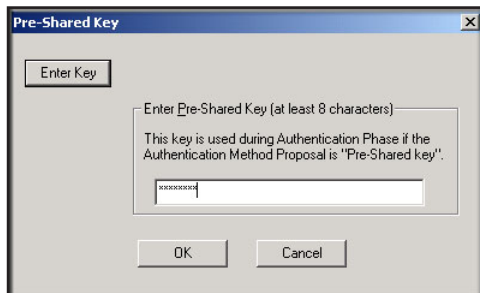
f. Click **Enter Key**. Enter the modem router pre-shared key, and then click **OK**. In this example, 12345678 is entered, though asterisks are displayed in the field. This field is case-sensitive.

5. Configure the VPN client authentication proposal.

In this step, you provide the type of encryption (DES or 3DES) to be used for this connection. This selection has to match your selection in the modem router configuration.

a. In the Network Security Policy list on the left side of the Security Policy Editor window, expand the Security Policy heading by double-clicking its name or clicking the + symbol.

b. Expand the Authentication subheading by double-clicking its name or clicking the + symbol. Then click **Proposal 1** below Authentication.
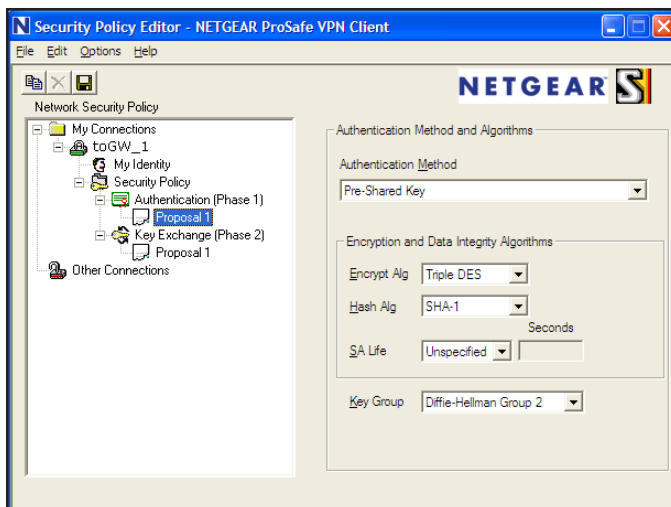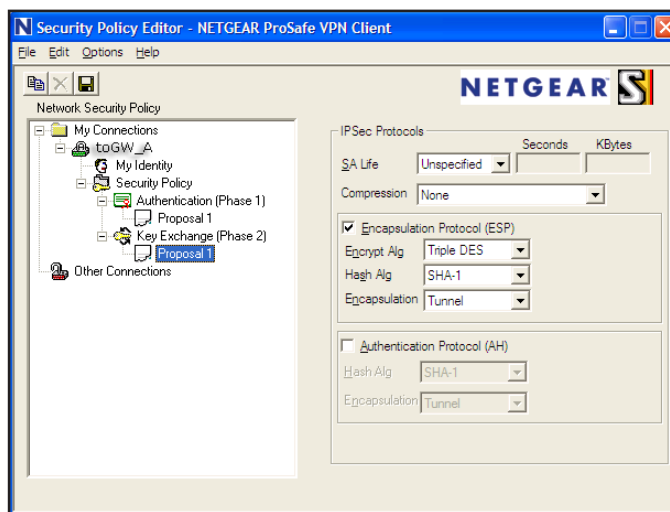

c. In the Authentication Method drop-down list, select **Pre-Shared key**.

d. In the Encrypt Alg drop-down list, select the type of encryption that is configured for the Encryption Protocol in the modem router in *Table 4* on page 96. This example uses Triple DES.

e. In the Hash Alg drop-down list, select **SHA-1**.

f. In the SA Life drop-down list, select **Unspecified**.

g. In the Key Group drop-down list, select **Diffie-Hellman Group 2**.

6. Configure the VPN client key exchange proposal.

In this step, you provide the type of encryption (DES or 3DES) to be used for this connection. This selection has to match your selection in the modem router configuration.

a. Expand the Key Exchange subheading by double-clicking its name or clicking the + symbol. Then click **Proposal 1** below Key Exchange.

b. In the SA Life drop-down list, select **Unspecified**.

c. In the Compression drop-down list, select **None**.

d. Select the **Encapsulation Protocol (ESP)** check box.

e. In the Encrypt Alg drop-down list, select the type of encryption that is configured for the encryption protocol in the modem router in *Table 4* on page 96. This example uses Triple DES.

f. In the Hash Alg drop-down list, select **SHA-1**.

g. In the Encapsulation drop-down list, select **Tunnel**.

h. Leave the **Authentication Protocol (AH)** check box cleared.

7. Save the VPN client settings.

In the Security Policy Editor window, select **File > Save**.

After you have configured and saved the VPN client information, your PC automatically opens the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router's LAN.

8. Check the VPN connection.

To check the VPN connection, you can initiate a request from the remote PC to the modem router's network by using the Connect option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client reports the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address, it has to initiate the request.

To perform a ping test using our example, start from the remote PC:

a. Establish an Internet connection from the PC.

b. On the Windows taskbar, click the **Start** button, and then select **Run**.

c. Type `ping -t 192.168.3.1`, and then click **OK**.
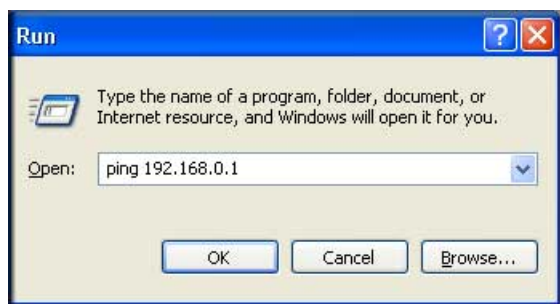
This causes a continuous ping to be sent to the first modem router. After between several seconds and 2 minutes, the ping response should change from timed out to reply.

Once the connection is established, you can open a browser on the PC and enter the LAN IP address of the remote gateway. After a short wait, you should see the login screen of the modem router (unless another PC is already logged in to the modem router).
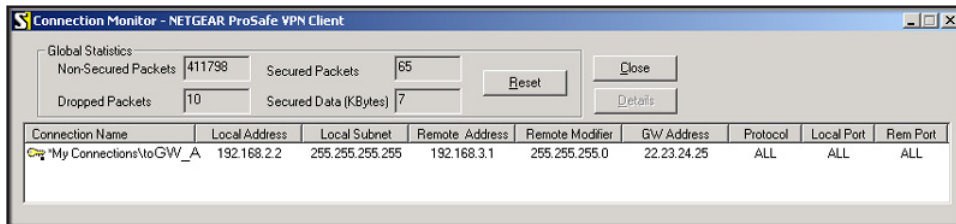
You can view information about the progress and status of the VPN client connection by opening the NETGEAR ProSafe Log Viewer.

To launch this function, click the Windows **Start** button, then select **Programs > NETGEAR ProSafe VPN Client > Log Viewer.** The Log Viewer screen for a successful connection is shown in this figure:

```
VPN Status/Log

Sun, 2002-09-08 12:01:35 - added connection description "fromDG834
Sun, 2002-09-08 12:01:35 - adding interface ipsec0/ppp0 67.116.6.4
Tue, 2005-05-24 20:46:33 - [fromGW_A ] responding to Main Mode fr
Tue, 2005-05-24 20:46:35 - [fromGW_A ] sent MR3, ISAKMP SA establ
Tue, 2005-05-24 20:46:35 - [fromGW_A ] responding to Quick Mode
Tue, 2005-05-24 20:46:36 - [fromGW_A ] IPsec SA established
Tue, 2005-05-24 20:50:41 - deleting connection "fromDG834G" instan
Tue, 2005-05-24 20:50:41 - deleting connection "fromDG834G"
Tue, 2005-05-24 20:50:41 - shutting down interface ipsec0/ppp0 67.
Tue, 2005-05-24 20:50:42 - added connection description "fromDG834
Tue, 2005-05-24 20:50:42 - adding interface ipsec0/ppp0 67.116.6.4

        Refresh      Clear Log     VPN Status
```

> **Note:** *Use the active VPN tunnel information and pings to determine whether a failed connection is due to the VPN tunnel or some reason outside the VPN tunnel.*

9. The Connection Monitor screen for this connection is shown in the following figure:

```
Connection Monitor - NETGEAR ProSafe VPN Client                      _ □ ×
 Global Statistics
   Non-Secured Packets  411798   Secured Packets   65        Close
                                                  Reset
   Dropped Packets      10       Secured Data (KBytes) 7      Details

Connection Name        Local Address  Local Subnet    Remote Address  Remote Modifier  GW Address   Protocol  Local Port  Rem Port
*My Connections\toGW_A  192.168.2.2   255.255.255.255 192.168.3.1     255.255.255.0    22.23.24.25  ALL       ALL         ALL
```

In this example you can see these settings:

- The modem router has a GW address (public IP WAN address) of 22.23.24.25.

- The modem router has a remote address (LAN IP address) of 192.168.3.1.

- The VPN client PC has a local address (dynamically assigned address) of 192.168.2.2.

While the connection is being established, the Connection Name field in this screen displays SA before the name of the connection. When the connection is successful, the SA changes to the yellow key symbol shown in the previous figure.

> **Note:** While your PC is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you have to close the VPN connection to have normal Internet access.

Set Up a Gateway-to-Gateway VPN Configuration

This section describes how to use the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in *Table 5* on page 97. If you have special requirements not covered by these VPNC-recommended parameters, see *Set Up VPN Tunnels in Special Circumstances* on page 116 for information about how to set up the VPN tunnel.

Follow this procedure to configure a gateway-to-gateway VPN tunnel using the VPN Wizard.
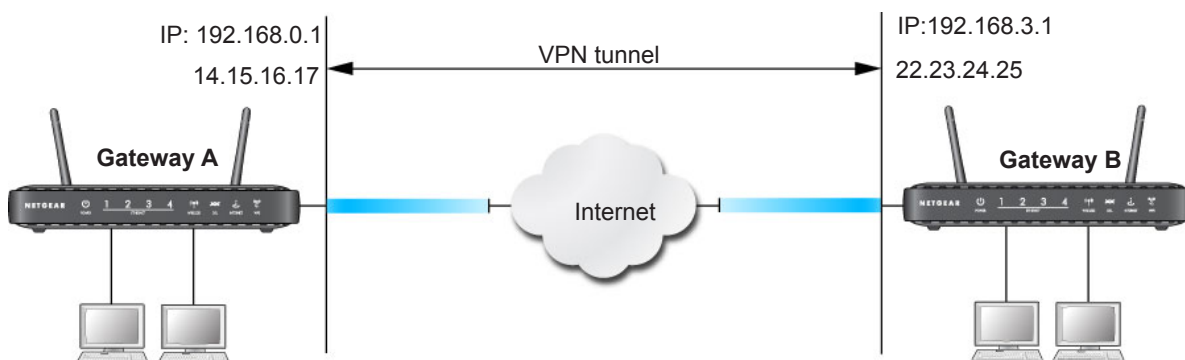
Figure 12. Gateway-to-gateway VPN tunnel

Set the LAN IPs on each modem router to a different subnet and configure each correctly for the Internet. The subsequent examples assume the settings shown in the following table.

Table 7. Gateway-to-Gateway VPN Tunnel Configuration Worksheet

Parameter		Value to Be Entered	Field Selection	
Connection Name		GtoGr	N/A	
Pre-Shared Key		12345678	N/A	
Secure Association		N/A	Main Mode	Manual Keys
Perfect Forward secrecy		N/A	Enabled	Disabled
Encryption Protocol		N/A	DES	3DES
Authentication Protocol		N/A	MD5	SHA-1
Diffie-Hellman (DH) Group		N/A	Group 1	Group 2
Key Life in seconds		28800 (8 hours)	N/A	
IKE Life Time in seconds		3600 (1 hour)	N/A	
VPN Endpoint	**Local IPSecID**	**LAN IP Address**	**Subnet Mask**	**FQDN or Gateway IP (WAN IP Address)**

Table 7. Gateway-to-Gateway VPN Tunnel Configuration Worksheet

Parameter		Value to Be Entered	Field Selection	
Gateway_A	GW_A	192.168.0.1	255.255.255.0	14.15.16.17
Gateway_B	GW_B	192.168.3.1	255.255.255.0	22.23.24.25

The LAN IP address ranges of each VPN endpoint have to be different. The connection will fail if both are using the NETGEAR default address range of 192.168.0.x.

➢ **To configure a gateway-to-gateway VPN tunnel using the VPN Wizard:**

1. Log in to Gateway A on LAN A.

2. Select **Advanced > Advanced - VPN > VPN Wizard**.
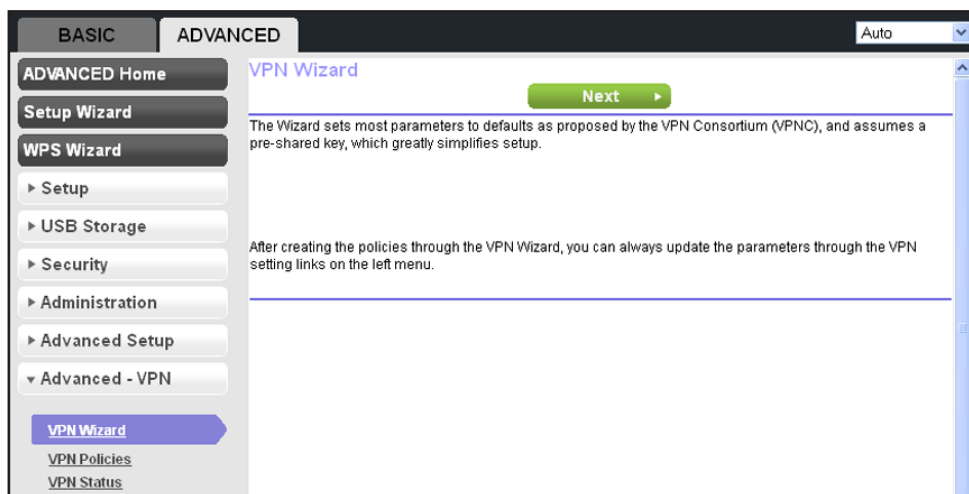
3. Click **Next**.

4. Fill in the Connection Name field and pre-shared key fields. Select the radio button for **A remote VPN Gateway**, and click **Next**.

5. Fill in the IP address or FQDN for the target VPN endpoint WAN connection, and click **Next**. The Step 3 screen displays.

6. Fill in the IP Address and Subnet Mask fields for the target endpoint that can use this tunnel, and click **Next**.

7. Specify the local LAN address and subnet mask, and click **Next**.

   The VPN Wizard Summary screen displays:

   To view the VPNC-recommended authentication and encryption settings used by the VPN Wizard, click the **here** link.

8. Click **Done** on the Summary screen.

9. The VPN Policies screen displays, showing that the new tunnel is enabled.

#	Enable	Name	Type	Local	Remote	ESP
1	✓	GtoClient	Auto	192.168.0.1 / 255.255.255.0	---	3DES
2	✓	GtoG	Auto	192.168.0.1 / 255.255.255.0	192.168.1.1 / 255.255.255.0	3DES

Note: *See Use Auto Policy to Configure VPN Tunnels on page 116 for information about how to enable the IKE keepalive capability on an existing VPN tunnel.*

10. Repeat these steps for the gateway on LAN B, and pay special attention to the following network settings:

   • WAN IP of the remote VPN gateway (for example, **14.15.16.17**)

   • LAN IP settings of the remote VPN gateway:

      - IP address (for example, **192.168.0.1**)

      - Subnet mask (for example, **255.255.255.0**)

      - Preshared key (for example, **12345678**)

11. Use the VPN Status screen to activate the VPN tunnel by performing the following steps:

   Note: The VPN Status screen is only one of three ways to active a VPN tunnel. See *Activate a VPN Tunnel* on page 112 for information about the other ways.

   a. Select **Advanced > Advanced - VPN > VPN Status**, and click the **VPN Status** button to display the Current VPN Tunnels (SAs) screen:

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	d90dc994	d924fef5	111	172.21.6.59	Drop	3549	3600

   b. Click **Connect** for the VPN tunnel you want to activate. View the VPN Status/Log screen to verify that the tunnel is connected.

VPN Tunnel Control

Activate a VPN Tunnel

There are three ways to activate a VPN tunnel:

• Use the VPN Status screen.

• Ping the remote endpoint.

• Start using the VPN tunnel.

Note: See *Use Auto Policy to Configure VPN Tunnels* on page 116 for information about how to enable the IKE keep-alive capability on an existing VPN tunnel.

Use the VPN Status Screen to Activate a VPN Tunnel

1. Select **Advanced > Advanced - VPN > VPN Status**, and click the **VPN Status** button to display the Current VPN Tunnels (SAs) screen:

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	d90dc994	d924fef5	111	172.21.6.59	Drop	3549	3600

2. Click **Connect** for the VPN tunnel that you want to activate.

Activate the VPN Tunnel by Pinging the Remote Endpoint

Note: This section uses 192.168.3.1 for sample remote endpoint LAN IP address.

To activate the VPN tunnel by pinging the remote endpoint (for example, 192.168.3.1), perform the following steps depending on whether your configuration is client-to-gateway or gateway-to-gateway:

• **Client-to-gateway configuration**. To check the VPN connection, you can initiate a request from the remote PC to the DGN2200v3's network by using the Connect option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client reports the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address, it has to initiate the request.

To perform a ping test using our example, start from the remote PC:

a. Establish an Internet connection from the PC.

b. On the Windows taskbar, click the **Start** button, and then select **Run**.

c. Type `ping -t 192.168.3.1,` and then click **OK**.
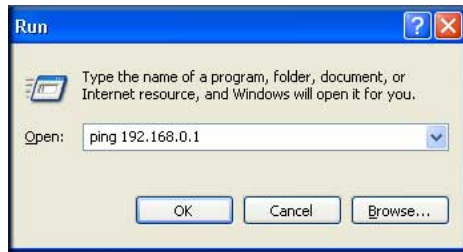
Running a ping test
to the LAN from the PC

This causes a continuous ping to be sent to the first DGN2200v3. Within 2 minutes, the ping response should change from timed out to reply.

Note: You can use Ctrl-C to stop the pinging.

Once the connection is established, you can open a browser on the PC and enter the LAN IP address of the remote DGN2200v3. After a short wait, you should see the login screen of the modem router (unless another PC already has the DGN2200v3 management interface open).

• **Gateway-to-gateway configuration**. Test the VPN tunnel by pinging the remote network from a PC attached to Gateway A (the modem router).

a. Open a command prompt (for example, **Start > Run > cmd**).

b. Type **ping 192.168.3.1**.

Note: The pings might fail the first time. If they do, then try the pings a second time.

Start Using a VPN Tunnel to Activate It

To use a VPN tunnel, use a Web browser to go to a URL whose IP address or range is covered by the policy for that VPN tunnel.

Verify the Status of a VPN Tunnel

1. Select **Advanced > Advanced - VPN > VPN Status**. The VPN Status/Log screen displays:

```
VPN Status/Log
        Refresh          Clear Log          VPN Status

2012-07-25 10:13:53 [=== Initiating PHASE 1 Main Mode (to 172.21.6
2012-07-25 10:13:53 ****** SENDING FIRST Main Mode PACKET (to 172.
2012-07-25 10:13:54 ****** RECEIVE PACKET PAYLOADS (SA,VID,VID)***
2012-07-25 10:13:54 ****** SENDING PACKET (to 172.21.6.59) ******
2012-07-25 10:13:54 ****** RECEIVE PACKET PAYLOADS (KE,NONCE)*****
2012-07-25 10:13:54 ****** SENDING PACKET (to 172.21.6.59) ******
2012-07-25 10:13:54 ****** RECEIVE PACKET PAYLOADS (ID,HASH)******
2012-07-25 10:13:54 ISAKMP SA established  (auth=OAKLEY_PRESHARED_
2012-07-25 10:13:54 [=== IKE PHASE 2 Quick Mode (to 172.21.6.59) =
2012-07-25 10:13:54 ****** SENDING FIRST Quick Mode PACKET (to 172
2012-07-25 10:13:54 ****** RECEIVE PACKET PAYLOADS (HASH,SA,NONCE,
2012-07-25 10:13:54 ****** SENDING PACKET (to 172.21.6.59) ******
2012-07-25 10:13:55 IPsec SA established  tunnel mode (ESP=>0xd90d
```

    This log shows the details of recent VPN activity, including the building of the VPN tunnel. If there is a problem with the VPN tunnel, refer to the log for information about what might be the cause of the problem.

    - Click **Refresh** to see the most recent entries.
    - Click **Clear Log** to delete all log entries.

2. Click the **VPN Status** button to display the Current VPN Tunnels (SAs) screen.

Current VPN Tunnels (SAs)

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	d90dc994	d924fef5	111	172.21.6.59	Drop	3549	3600

    This table lists the following data for each active VPN tunnel.

    - **SPI**. Each SA has a unique SPI (Security Parameter Index) for traffic in each direction. For manual key exchange, the SPI is specified in the policy definition. For automatic key exchange, the SPI is generated by the IKE protocol.
    - **Policy Name**. The VPN policy associated with this SA.
    - **Remote Endpoint**. The IP address on the remote VPN endpoint.
    - **Action**. Either a Drop or a Connect button.

- **SLifeTime (Secs)**. The remaining soft lifetime for this SA in seconds. When the soft lifetime becomes 0 (zero), the SA (security association) is re-negotiated.

- **HLifeTime (Secs)**. The remaining hard lifetime for this SA in seconds. When the hard lifetime becomes 0 (zero), the SA (security association) is terminated. (It is re-established if required.)

Deactivate a VPN Tunnel

Sometimes a VPN tunnel has to be deactivated for testing purposes. You can deactivate a VPN tunnel from two places:

- Policy table on VPN Policies screen
- VPN Status screen

➢ **To use the Policy Table to deactivate a VPN tunnel:**

1. Select **Advanced > Advanced - VPN > VPN Policies** to display the VPN Policies screen.

2. In the Policy Table, clear the **Enable** check box for the VPN tunnel that you want to deactivate, and then click **Apply**. (To reactivate the tunnel, select the **Enable** check box, and then click **Apply**.)

➢ **To use the VPN Status Screen to deactivate a VPN tunnel:**

1. **Advanced > Advanced - VPN > VPN Status**, and click the **VPN Status** button. The Current VPN Tunnels (SAs) screen displays:

2. Click **Drop** for the VPN tunnel that you want to deactivate.

Delete a VPN Tunnel

➢ **To deactivate a VPN tunnel:**

1. Select **Advanced > Advanced - VPN > VPN Policies** to display the VPN Policies screen.

2. In the Policy Table, select the radio button for the VPN tunnel to be deleted and click **Delete**.

Set Up VPN Tunnels in Special Circumstances

When the VPN Wizard and its VPNC defaults (see *Table 5* on page 97) are not appropriate for your circumstances, use one of these alternatives:

- **Auto Policy**. For a typical automated Internet Key Exchange (IKE) setup, see *Use Auto Policy to Configure VPN Tunnels* on page 116. Auto Policy uses the IKE protocol to define the authentication scheme and automatically generate the encryption keys.

- **Manual Policy**. For a manual keying setup in which you have to specify each phase of the connection, see *Use Manual Policy to Configure VPN Tunnels* on page 123. Manual policy does not use IKE. Rather, you manually enter all the authentication and key parameters. You have more control over the process; however, the process is more complex, and there are more opportunities for errors or configuration mismatches between your DGN2200v3 and the corresponding VPN endpoint gateway or client workstation.

Use Auto Policy to Configure VPN Tunnels

You need to configure matching VPN settings on both VPN endpoints. The outbound VPN settings on one end have to match to the inbound VPN settings on other end, and vice versa.

See *Example of Using Auto Policy* on page 120 for an example of using Auto Policy.

Configure VPN Network Connection Parameters

All VPN tunnels on the modem router require that you configure several network parameters. This section describes those parameters and how to access them.

The most common configuration scenarios use IKE to manage the authentication and encryption keys. The IKE protocol performs negotiations between the two VPN endpoints to generate and update the required encryption parameters.

Select **Advanced > Advanced - VPN > VPN Policies**, and click the **Add Auto Policy** button to display the VPN - Auto Policy screen:

The DGN2200v3 VPN tunnel network connection fields are defined in the following sections.

VPN Auto Policy General Settings

- **Policy Name**. Enter a unique name. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.

- **Remote VPN Endpoint**. The remote VPN endpoint has to have this VPN gateway's address entered as its remote VPN endpoint.

  If the remote endpoint has a dynamic IP address, select **Dynamic IP Address**. No address data input is required. You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time. Otherwise, select an option (**IP address** or **domain name**) and enter the address of the remote VPN endpoint to which you want to connect.

- **IKE Keep Alive**. If you want to ensure that a connection is kept open, or, if that is not possible, that it is quickly re-established when a connection is lost select this check box.

  The ping IP address has to be associated with the remote endpoint. You have to use the remote LAN address. This IP address will be pinged periodically to generate traffic for the VPN tunnel. The remote keep-alive IP address needs to be covered by the remote LAN IP range and to correspond to a device that can respond to a ping. The range should be made as narrow as possible to meet this objective.

VPN Auto Policy Local LAN Settings

The remote VPN endpoint needs to have these IP addresses entered as its remote addresses.

- **Subnet Mask**. The network mask.

- **Single/Start IP Address**. Enter the IP address for a single address, or the starting address for an address range. A single address setting is used when you want to make a single server on your LAN available to remote users. A range has to be an address range used on your LAN. **Any**. The remote VPN endpoint might be at any IP address.
- **Finish IP Address**. For an address range, enter the finish IP address. This needs to be an address range used on your LAN.

VPN Auto Policy Remote LAN Settings

The remote VPN endpoint has to have these IP addresses entered as its local addresses.

- **IP Address**. If there is no LAN (only a single PC) at the remote endpoint, select **Single PC - no Subnet** option. If this option is selected, no additional data is required. The typical application is a PC running the VPN client at the remote end.
- **Single/Start IP Address**. Enter an IP address that is on the remote LAN. You can use this setting when you want to access a server on the remote LAN.
    - For a range of addresses, enter the starting IP address. This needs to be an address range used on the remote LAN.
    - **Any**. Any outgoing traffic from the computers in the **Local IP** fields triggers an attempted VPN connection to the remote VPN endpoint. Be sure you want this option before selecting it.
- Finish IP Address. Enter the finish IP address for a range of addresses. This has to be an address range used on the remote LAN.
- Subnet Mask. Enter the network mask.

VPN Auto Policy IKE Settings

- **Direction**. This setting is used when the modem router determines if the IKE policy matches the current traffic. Select an option.
    - **Responder only**. Incoming connections are allowed, but outgoing connections are blocked.
    - **Initiator and Responder**. Both incoming and outgoing connections are allowed.
- **Exchange Mode**. Ensure that the remote VPN endpoint is set to use Main Mode.
- **Diffie-Hellman (DH) Group**. The Diffie-Hellman algorithm is used when keys are exchanged. The DH Group setting determines the bit size used in the exchange. This value needs to match the value used on the remote VPN gateway.
- **Local Identity Type**. Select an option to match the Remote Identity Type setting on the remote VPN endpoint.
    - **WAN IP Address**. Your Internet IP address.
    - **Fully Qualified Domain Name**. Your domain name.
    - **Fully Qualified User Name**. Your name, email address, or other ID.
    - **Local Identity Data**. Enter the data for the local identity type that you selected. (If WAN IP Address is selected, no input is required.)

- **Remote Identity Type**. Select the option that matches the Local Identity Type setting on the remote VPN endpoint.

  - **IP Address**. The Internet IP address of the remote VPN endpoint.

  - **Fully Qualified Domain Name**. The domain name of the remote VPN endpoint.

  - **Fully Qualified User Name**. The name, email address, or other ID of the remote VPN endpoint.

  - **Remote Identity Data**. Enter the data for the remote identity type that you selected. If IP Address is selected, no input is required.

VPN Auto Policy Parameters

- **Encryption Algorithm**. The encryption algorithm used for both IKE and IPSec. This setting has to match the setting used on the remote VPN gateway. DES and 3DES are supported.

  - **DES**. The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56-bit key. Faster but less secure than 3DES.

  - **3DES**. (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.

- **Authentication Algorithm**. The authentication algorithm used for both IKE and IPSec. This setting has to match the setting used on the remote VPN gateway. Auto, MD5, and SHA-1 are supported. Auto negotiates with the remote VPN endpoint and is not available in responder-only mode.

  - **MD5**. 128 bits, faster but less secure.

  - **SHA-1**. 160 bits, slower but more secure. This is the default.

- **Pre-shared Key**. The key has to be entered both here and on the remote VPN gateway.

- **SA Life Time**. The time interval before the SA (security association) expires. (It is automatically reestablished as required.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA life time. This setting applies to both IKE and IPSec SAs.

- **Enable IPSec PFS (Perfect Forward Secrecy)**. If this check box is selected, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.)

  This setting applies to both IKE and IPSec SAs. When configuring the remote endpoint to match this setting, you might have to specify the key group used. For this device, the key group is the same as the DH Group setting in the IKE section.

Example of Using Auto Policy

IP: 192.168.0.1

14.15.16.17

VPN Tunnel

IP:192.168.3.1

22.23.24.25

Gateway A

Internet
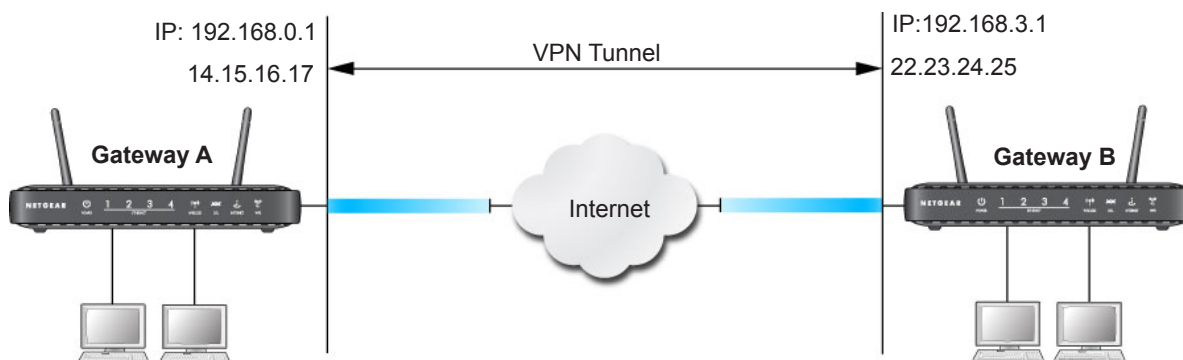
Gateway B

Figure 13. Auto Policy for a Gateway-to-Gateway tunnel

The following settings are assumed for this example:.

Table 8. Gateway-to-Gateway VPN Tunnel Configuration Worksheet

Parameter		Value to Be Entered	Field Selection	
Connection Name		GtoG	N/A	
Pre-Shared Key		12345678	N/A	
Secure Association		N/A	Main Mode	Manual Keys
Perfect Forward secrecy		N/A	Enabled	Disabled
Encryption Protocol		N/A	DES	3DES
Authentication Protocol		N/A	MD5	SHA-1
Diffie-Hellman (DH) Group		N/A	Group 1	Group 2
Key Life in seconds		28800 (8 hours)	N/A	
IKE Life Time in seconds		3600 (1 hour)	N/A	
VPN Endpoint	Local IPSecID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address
Gateway_A	GW_A	192.168.0.1	255.255.255.0	14.15.16.17
Gateway_B	GW_B	192.168.3.1	255.255.255.0	22.23.24.25

➢ **To use Auto Policy:**

1. Set the LAN IPs on each modem router to different subnets and configure each correctly for the Internet.

2. Select **Advanced - VPN > VPN Policies** and click the **Add Auto Policy** button.

The VPN Auto Policy screen displays:

3. Enter these policy settings:

Auto Policy Field		Description
General	Policy Name	GtoG
	Remote VPN Endpoint Address Type	Fixed IP Address
	Remote VPN Endpoint Address Data	22.23.24.25
Local LAN		Use the default settings.
Remote LAN	IP Address	Select **Subnet address** from the drop-down list.
	Single/Start IP Address	192.168.3.1
	Subnet Mask	255.255.255.0
IKE	Direction	Initiator and Responder
	Exchange Mode	Main Mode
	Diffie-Hellman (DH) Group	Group 2 (1024 Bit)
	Local Identity Type	Use the default setting.
	Remote Identity Type	Use the default setting.
Parameters	Encryption Algorithm	3DES
	Authentication Algorithm	MD5
	Pre-shared Key	12345678

4. Click **Apply**. The VPN Policies screen displays:

5. Repeat these steps for the DGN2200v3 on LAN B. Pay special attention to the following network settings:

- General, Remote Address Data (for example, 14.15.16.17)
- Remote LAN, Start IP Address
  - IP Address (for example, 192.168.0.1)
  - Subnet Mask (for example, 255.255.255.0)
  - Pre-shared Key (for example, 12345678)

6. Use the VPN Status screen to activate the VPN tunnel:

> **Note:** The VPN Status screen is only one of three ways to active a VPN tunnel. See *Activate a VPN Tunnel* on page 112 for information about the other ways.

a. Select **VPN > VPN Status** to display the VPN Status/Log screen. Then click **VPN Status** to display the Current VPN Tunnels (SAs) screen:

b. Click **Connect** for the VPN tunnel that you want to activate. Review the VPN Status/Log screen to verify that the tunnel is connected.

Use Manual Policy to Configure VPN Tunnels

As an alternative to IKE, you can use manual keying, in which you need to specify each phase of the connection. A manual VPN policy requires all settings for the VPN tunnel to be manually input at each end (both VPN endpoints).

Select **Advanced - VPN > VPN Policies**, and then click the **Add Manual Policy** radio button to display the VPN - Manual Policy screen:

The following sections explain the fields in the VPN Manual Policy screen.

VPN Manual Policy General Settings

The DGN2200v3 VPN tunnel network connection fields are as follows.

- **Policy Name**. Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.

- **Remote VPN Endpoint**. The remote VPN endpoint has to have this VPN gateway's address entered as its remote VPN endpoint.

  If the remote endpoint has a dynamic IP address, select **Dynamic IP Address**. No address data input is required. You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time. Otherwise, select an option (**IP address** or **domain name**) and enter the address of the remote VPN endpoint to which you want to connect.

VPN Manual Policy Local LAN Settings

The remote VPN endpoint has to have these IP addresses entered as its remote addresses.

- **Subnet Address**. Enter the network mask.
- **Single PC - no Subnet**. Select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required.

- **Single/Start IP Address**. The IP address for a single address, or the starting address for an address range used on the LAN. If you want to make a single server on your LAN available to remote users, use a single address Any settings. The remote VPN endpoint can be at any IP address.

- **Finish IP Address**. For an address range, enter the finish IP address. This has to be an address range used on your LAN.

- **Subnet Mask**. Enter the network mask.

VPN Manual Policy Remote LAN Settings

The remote VPN endpoint has to have these IP addresses entered as its local addresses.

- **IP Address**. Select **Single PC - no Subnet** if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required. The typical application is a PC running the VPN client at the remote end.

- **Single/Start IP Address**. Enter an IP address on the remote LAN. You can use this setting to access a server.

  - For a range of addresses, enter the starting IP address. This has to be an address range used on the remote LAN.

  - **Any**. Any outgoing traffic from specified Local IP computers triggers an attempted VPN connection to the remote VPN endpoint. Be sure you want this option before selecting it.

- **Finish IP Address**. Enter the finish IP address for a range of addresses. This has to be an address range used on the remote LAN.

- **Subnet Mask**. Enter the network mask.

VPN Manual Policy ESP Settings

ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel.

- **SPI**. Enter the required Security Policy Indexes (SPIs). Each policy has to have unique SPIs. These settings need to match the remote VPN endpoint. The **in** setting here has to match the **out** setting on the remote VPN endpoint, and the **out** setting here has to match the **in** setting on the remote VPN endpoint.

- **Encryption**. Select an encryption algorithm, and enter the key in the field provided. For 3DES, the keys should be 24 ASCII characters, and for DES, the keys should be 8 ASCII characters.

  - **DES**. The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56-bit key. Faster but less secure than 3DES.

  - **3DES**. (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.

- **Authentication**. Specify the authentication and the key.

Troubleshooting

10

Diagnosing and Solving Problems

This chapter provides information to help you diagnose and solve problems you might have with your modem router. If you do not find the solution here, check the NETGEAR support site at *http://support.netgear.com* for product and contact information.

This chapter contains the following sections:

- *Troubleshooting with the LEDs*
- *Troubleshooting the Internet Connection*
- *TCP/IP Network Not Responding*
- *Changes Not Saved*
- *Incorrect Date or Time*

Troubleshooting with the LEDs

When you turn the power on, the power, LAN, and DSL LEDs should light as described here. If they do not, refer to the sections that follow for help.

1. When power is first applied, the Power LED lights.
2. After approximately 10 seconds, the LAN and DSL LEDs light as follows:
   a. The LAN port LEDs light for any local ports that are connected.
   b. The DSL link LED lights to indicate that there is a link to the connected device.
   c. If a LAN port is connected to a 100 Mbps device, verify that the LAN port's LED is green. If the LAN port is 10 Mbps, the LED is amber.
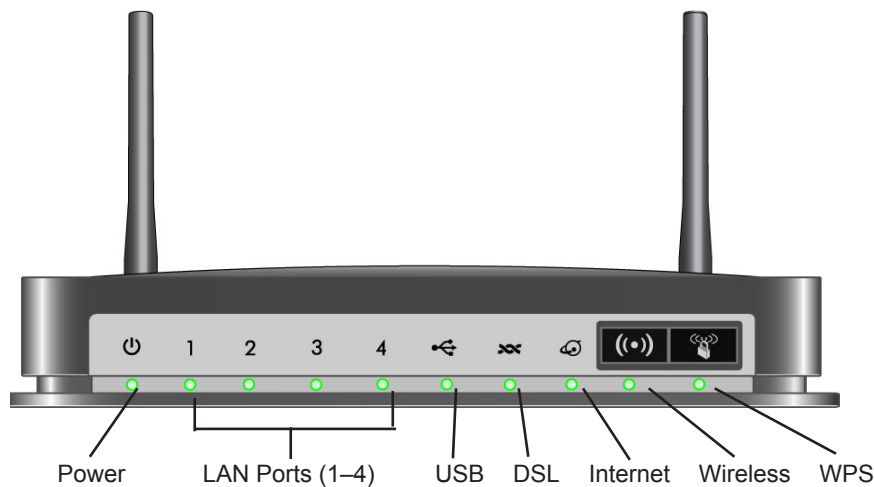
Figure 14. Front panel LEDs

Power LED Is Off

If the Power and other LEDs are off when your modem router is turned on:

- Check that the power cord is correctly connected to your modem router and the power supply adapter is correctly connected to a functioning power outlet.
- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

If the error persists, you could have a hardware problem and should contact NETGEAR Technical Support.

Power LED Is Red

When the modem router is turned on, it performs a power-on self-test during which time the Power LED turns red. If the Power LED does not turn green within a minute or so or if it turns red at any other time during normal operation there is a fault within the modem router.

If the Power LED turns red to indicate a modem router fault, turn the power off and on to see if the modem router recovers. If the power LED is still red 1 minute after power-up:

* Turn the power off and on one more time to see if the modem router recovers.

* Clear the modem router's configuration to factory defaults as explained in *Factory Settings* on page 134. This sets the modem router's IP address to 192.168.0.1.

If the error persists, you could have a hardware problem and should contact NETGEAR Technical Support.

LAN LED Is Off

If the appropriate LAN LED does not light when the Ethernet connection is made, check the following:

* The Ethernet cable connections are secure at the modem router and at the hub or workstation.

* The power is turned on to the connected hub or workstation.

* You are using the correct cable.

Cannot Log In to the Modem Router

If you are unable to log in to the modem router from a computer on your local network, check the following:

* If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the modem router as described in the previous section.

* Make sure that your computer's IP address is on the same subnet as the modem router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254.

* If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and MacOS generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the modem router, and reboot your computer.

* If your modem router's IP address was changed and you do not know the current IP address, clear the modem router's configuration to factory defaults. This sets the modem router's IP address to 192.168.0.1. This procedure is explained in *Factory Settings* on page 134.

* Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.

* Try quitting the browser and launching it again.

* Make sure you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.

Troubleshooting the Internet Connection

If your modem router is unable to access the Internet, check the ADSL connection, then the WAN TCP/IP connection.

ADSL Link

If your modem router is unable to access the Internet, first determine whether you have an ADSL link with the service provider. The state of this connection is indicated with the Internet LED.

ADSL Link LED Is Green

If your ADSL link LED is green, then you have a good ADSL connection. You can be confident that the service provider has connected your line correctly and that your wiring is correct.

ADSL Link LED Is Blinking Green

If your ADSL link LED is blinking green, then your modem router is attempting to make an ADSL connection with the service provider. The LED should turn green within several minutes.

If the ADSL link LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green ADSL link LED, there might be a problem with your wiring. If the telephone company has tested the ADSL signal at your network interface device (NID), then you might have poor-quality wiring in your house.

ADSL Link LED Is Off

If the ADSL link LED is off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green ADSL link LED, check for the following:

• Check that the telephone company has made the connection to your line and tested it.

• Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It might be necessary to use a swapper if your ADSL signal is on pins 1 and 4 or the RJ-11 jack. The modem router uses pins 2 and 3.

Internet LED Is Red

If the Internet LED is red, the device was unable to connect to the Internet. Verify the following:

- Check that your login credentials are correct, or that the information you entered on the Basic Settings screen is correct.
- Check with your ISP to verify that the multiplexing method, VPI, and VCI settings on the ADSL settings screen are correct.
- Check if your ISP has a problem—it might not be that the modem router cannot connect to the Internet but, rather that your ISP that cannot provide an Internet connection.

Obtaining an Internet IP Address

If your modem router is unable to access the Internet, and your Internet LED is green, see if the modem router can obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your modem router requests an IP address from the ISP. You can determine whether the request was successful using the browser interface.

➢ **To check the Internet IP address from the browser interface:**

1. Launch your browser, and select an external site such as *www.netgear.com*.
2. Access the main menu of the modem router's configuration at http://192.168.0.1.
3. In the main menu, under Maintenance, select **Router Status** and check that an IP address is shown for the WAN port. If 0.0.0.0 is shown, your modem router has not obtained an IP address from your ISP.

If your modem router is unable to obtain an IP address from the ISP, the problem might be one of the following:

- If you have selected a login program, the service name, user name, or password might be incorrectly set. See the following section, *Troubleshooting PPPoE or PPPoA* .
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account to the modem router in the browser-based Setup Wizard.
- Your ISP allows only one Ethernet MAC address to connect to Internet, and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the modem router's MAC address.
  - Configure your modem router to spoof your computer's MAC address. This can be done in the Basic Settings screen.

Troubleshooting PPPoE or PPPoA

➢ **To debut the PPPoE or PPPoA connection:**

1. Access the main menu of the modem router at http://192.168.0.1.
2. Select **Maintenance > Router Status**.

3. Click the **Connection Status** button.

4. If all of the steps indicate OK, then your PPPoE or PPPoA connection is up and working.

5. If any of the steps indicates Failed, you can attempt to reconnect by clicking **Connect**. The modem router continues to attempt to connect indefinitely.

If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There also might be a provisioning problem with your ISP.

> **Note:** Unless you connect manually, the modem router does not authenticate using PPPoE or PPPoA until data is transmitted to the network.

Troubleshooting Internet Browsing

If your modem router can obtain an IP address, but your computer is unable to load any Web pages from the Internet:

*   Your computer might not recognize any DNS server addresses.

    A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address when you set up the modem router, reboot your computer, and verify the DNS address. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

*   Your computer might not have the modem router configured as its TCP/IP modem router.

    If your computer obtains its information from the modem router by DHCP, reboot the computer, and verify the modem router address.

TCP/IP Network Not Responding

Most TCP/IP terminal devices and routers have a ping utility for sending an echo request packet to the designated device. The device responds with an echo reply to tell whether a TCP/IP network is responding to requests.

Test the LAN Path to Your Modem Router

You can ping the modem router from your computer to verify that the LAN path to your modem router is set up correctly.

➢ **To ping the modem router from a PC running Windows 95 or later:**

1. From the Windows task bar, click the **Start** button, and select **Run**.

2. In the field provided, type **ping** followed by the IP address of the modem router, as in this example:

   ping 192.168.0.1

3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

   If the path is working, you see this message:

   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you see this message:

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you could have one of the following problems:

   - Wrong physical connections
     - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in *LAN LED Is Off* on page 127.
     - Check that the corresponding link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and modem router.

   - Wrong network configuration
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
     - Verify that the IP address for your modem router and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After you verify that the LAN path works correctly, test the path from your PC to a remote device. In the Windows Run screen, type:

```
ping -n 10 IP address
```

where *IP address* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as described in *Test the LAN Path to Your Modem Router* on page 130 display. If you do not receive replies:

- Check that your PC has the IP address of your modem router listed as the default modem router. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel. Verify that the IP address of the modem router is listed as the default router.

- Check that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.

- Check that your cable or DSL modem is connected and functioning.

- If your ISP assigned a host name to your PC, enter that host name as the account name in the Basic Settings screen.

- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your modem, but some additionally restrict access to the MAC address of a single PC connected to that modem. In this case, configure your modem router to clone or spoof the MAC address from the authorized PC.

Changes Not Saved

If the modem router does not save the changes you make in the modem router interface, check the following:

- When entering configuration settings, always click the **Apply** button before moving to another screen or tab, or your changes are lost.

- Click the **Refresh** or **Reload** button in the Web browser. The changes might have occurred, but the old settings might be in the Web browser's cache.

Incorrect Date or Time

Select **Security > Schedule** to display the current date and time. The modem router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2000. This means the modem router has not yet reached a network time server. Check that your Internet access is configured correctly. If you have just finished setting up the modem router, wait at least 5 minutes, and check the date and time again.

- Time is off by one hour. This modem has automatic DST adjustment. To use this feature, in the Schedule screen, make sure this check box is checked: **Automatically adjust for daylight savings time**.

Supplemental Information

A

This appendix includes the factory default settings and technical specifications for the N300 Wireless ADSL2+ Modem Router DGN2200v3, and instructions for wall-mounting the unit.

This appendix contains the following sections:

- *Factory Settings*
- *Specifications*

Factory Settings

You can return the modem router to its factory settings. On the bottom of the modem router, use the end of a paper clip or some other similar object to press and hold the Restore Factory Settings button ⬡ for at least 7 seconds. The modem router resets, and returns to the factory settings. Your device will return to the factory configuration settings shown in the following table.

Table 9. Factory Default Settings

Feature		Default Behavior
Router Login	User login URL	www.routerlogin.com or /www.routerlogin.net
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default address
	WAN MTU size	1492
	Port speed	Autosensing
Local network (LAN)	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled
Local network (LAN) continued	DHCP starting IP address	192.168.0.2
	DHCP ending IP address	192.168.0.254
	DMZ	Enabled or disabled
	Time zone	GMT for WW except NA and GR, GMT+1 for GR, GMT-8 for NA
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled

Table 9. Factory Default Settings (continued)

Feature		Default Behavior
Wireless	Wireless communication	Enabled
	SSID name	Can be found on the label on the bottom of the unit.
	Security	Can be found on the label on the bottom of the unit.
	Broadcast SSID	Enabled
	Country/region	United States (in North America; otherwise, varies by region)
	RF channel	Auto
	Operating mode	Up to 145 Mbps
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Pre-Shared Key
	Wireless card access list	All wireless stations allowed

Specifications

Table 10.

Specification	Description
Network protocol and standards compatibility	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power adapter	North America: 120V, 60 Hz, input
	UK, Australia: 240V, 50 Hz, input
	Europe: 230V, 50 Hz, input
	All regions (output): 12V @ 1A output
Physical	Dimensions: 6.80 in. x 5.03 in. x 1.28 in. (173 mm x 128 mm x 33 mm)
	Weight: 0.65 lbs. without the stand (0.29 kg)
Environmental	Operating temperature: 0° to 40° C (32° to 104° F)
	Operating humidity: 10% to 90% relative humidity, noncondensing
	Storage temperature: –20° to 70° C (–4° to 158° F)
	Storage humidity: 5 to 95% relative humidity, noncondensing
Regulatory compliance	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B
Network protocol and standards compatibility	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power adapter	North America: 120V, 60 Hz, input
Regulatory compliance	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B
Interface specifications	LAN: 10BASE-T or 100BASE-Tx, RJ-45 WAN: ADSL, Dual RJ-11, pins 2 and 3 T1.413, G.DMT, G.Lite ITU Annex A hardware or Annex B hardware ITU G.992.5 (ADSL2+)

VPN Configuration

IPSec VPN tunnel

B

This appendix is a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR DGN2200v3 to a FVL328. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

This appendix contains the following sections:

- *Configuration Profile*
- *Modem Router with FQDN to Gateway B*
- *Configuration Summary (Telecommuter Example)*
- *Setting Up Client-to-Gateway VPN Configuration*
- *Monitoring the VPN Tunnel*

Configuration Profile

The configuration in this appendix follows the addressing and configuration mechanics defined by the VPN Consortium. Gather necessary information before you begin configuration. Verify that the firmware is up to date, and that you have all the addresses and parameters to be set on both sides. Check that there are no firewall restrictions.

Table 11.

VPN Consortium Scenario	Scenario 1 (Identity Using Preshared Secrets)
Type of VPN	LAN-to-LAN or gateway-to-gateway (not PC/client-to-gateway)
Security scheme:	IKE with preshared secret/key (not certificate based)
IP addressing:	
NETGEAR-Gateway A	Static IP address
NETGEAR-Gateway B	Static IP address
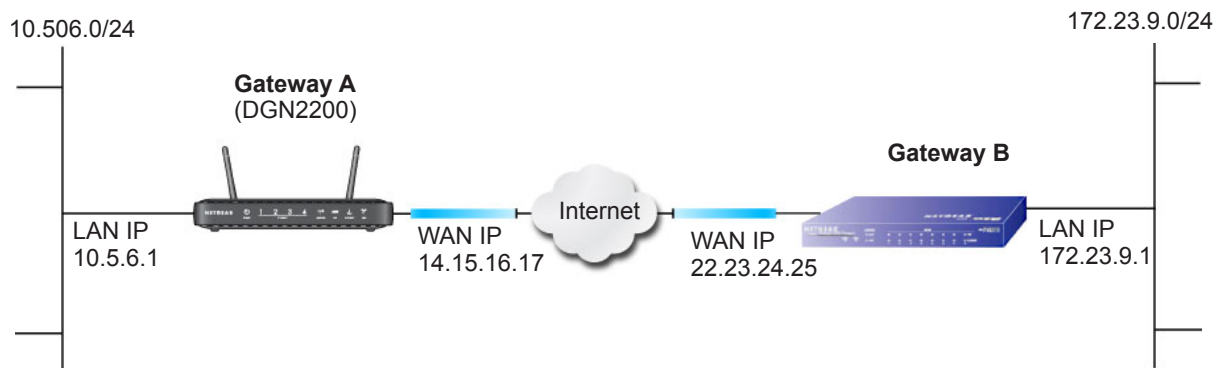
Figure 15. VPNC Example, Network Interface Addressing

Step-by-Step Configuration

1. Use the VPN Wizard to configure Gateway A (DGN2200v3) for a gateway-to-gateway tunnel (see *Set Up a Gateway-to-Gateway VPN Configuration* on page 108), being certain to use appropriate network addresses for the environment.

    The LAN addresses used in this example are as follows:

Unit	WAN IP	LAN IP	LAN Subnet Mask
DGN2200v3	14.15.16.17	10.5.6.1	255.255.255.0
FVL328	22.13.24.25	172.23.9.1	255.255.255.0

    a. Enter **toGW_B** for the connection name.

VPN Configuration

    b. Enter **22.23.24.25** for the remote WAN's IP address.

    c. Enter the following:

- IP Address. **172.23.9.1**
- Subnet Mask. **255.255.255.0**

    d. In the Summary screen, click **Done**.

2. Use the VPN Wizard to configure the Gateway B for a gateway-to-gateway tunnel (see *Set Up a Gateway-to-Gateway VPN Configuration* on page 108), being certain to use appropriate network addresses for the environment.

    a. Enter **toGW_A** for the connection name.

    b. Enter **14.15.16.17** for the remote WAN's IP address.

    c. Enter the following:

- IP Address. **10.5.6.1**
- Subnet Mask. **255.255.255.0**

    d. In the Summary screen, click **Done**.

3. On the Gateway B router menu, under VPN, select IKE Policies, and click the **Edit** button to display the IKE Policy Configuration screen:

4. On Gateway B router menu, under VPN, select VPN Policies, and click the **Edit** button to display the VPN Auto Policy screen:

5. Test the VPN tunnel by pinging the remote network from a PC attached to Gateway A (modem router).

   a. Open the command prompt (Start > Run > cmd).

   b. Type `ping 172.23.9`.

   If the pings fail the first time, try the pings a second time.

Modem Router with FQDN to Gateway B

This section is a case study on how to configure a VPN tunnel from a NETGEAR modem router to a gateway using a fully qualified domain name (FQDN) to resolve the public address of one or both routers. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

Configuration Profile

The configuration in this section follows the addressing and configuration mechanics defined by the VPN Consortium. Gather the necessary information before you begin configuration. Verify that the firmware is up to date, and that you have all the addresses and parameters to be set on both sides. Check that there are no firewall restrictions.
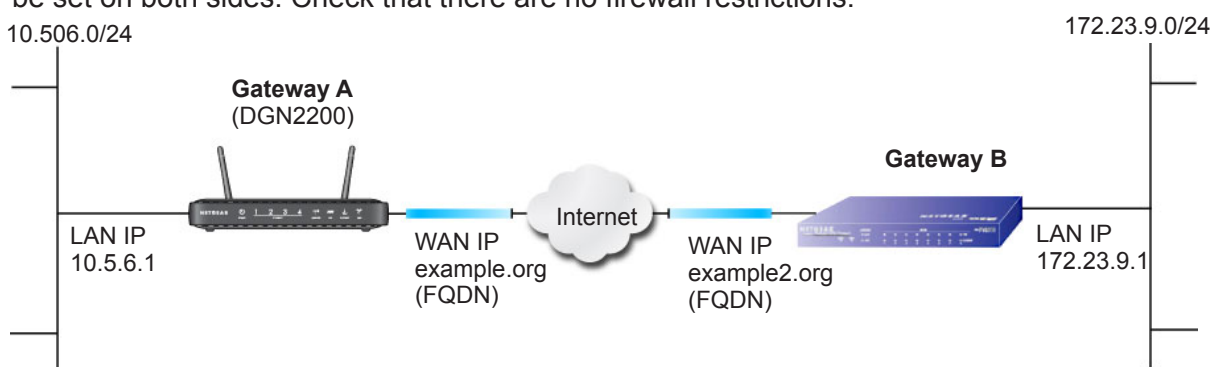
Figure 16. VPNC Example, Network Interface Addressing

VPN Consortium Scenario	Scenario 1
Type of VPN	LAN-to-LAN or gateway-to-gateway (not PC/client-to-gateway)
Security scheme:	IKE with preshared secret/Key (not certificate based)
IP addressing:	
NETGEAR-Gateway A	Fully qualified domain name (FQDN)
NETGEAR-Gateway B	FDQN

Using a Fully Qualified Domain Name (FQDN)

Many ISPs provide connectivity to their customers using dynamic instead of static IP addressing. This means that a user's IP address does not remain constant over time, which presents a challenge for gateways attempting to establish VPN connectivity.

A Dynamic DNS (DDNS) service allows a user whose public IP address is dynamically assigned to be located by a host or domain name. It provides a central public database where information (such as e-mail addresses, host names, and IP addresses) can be stored and retrieved. Now, a gateway can be configured to use a third-party service instead of a permanent and unchanging IP address to establish bi-directional VPN connectivity.

To use DDNS, you need to register with a DDNS service provider. Some DDNS service providers include:

- DynDNS: www.dyndns.org
- TZO.com: netgear.tzo.com
- ngDDNS: ngddns.iego.net

In this example, Gateway A is configured using a sample FQDN provided by a DDNS service provider. In this case we established the hostname **dg834g.dyndns.org** for Gateway A using the DynDNS service. Gateway B uses the DDNS service provider when establishing a VPN tunnel.

To establish VPN connectivity, Gateway A has to be configured to use Dynamic DNS, and Gateway B has to be configured to use a DNS host name provided by a DDNS service provider to find Gateway A. Again, the following step-by-step procedures assume that you have already registered with a DDNS service provider and have the configuration information necessary to set up the gateways.

Step-by-Step Configuration

1. Log in to Gateway A (your modem router).

   This example assumes that you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.

2. On Gateway A, configure the Dynamic DNS settings.

   a. On the Advanced tab, select **Advanced Setup > Dynamic DNS** to display the following screen:

   b. Fill in the fields with account and host name settings.
      - Select the **Use a Dynamic DNS Service** check box.
      - In the **Host Name** field, type **gw_a.dyndns.org**.
      - In the **User Name** field, enter the account user name.
      - In the **Password** field, enter the account password.

   c. Click **Apply**.

d. Click **Show Status**. The resulting screen should show Update OK: good:
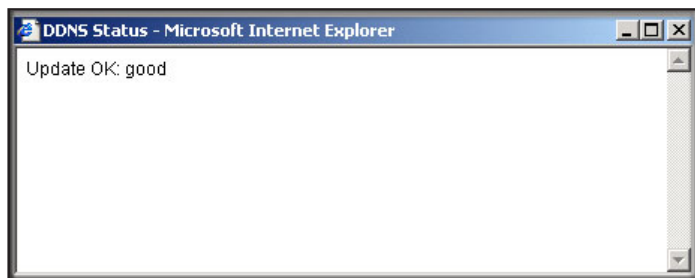
3. On Gateway B, configure the Dynamic DNS settings. Assume a correctly configured DynDNS account.

a. From the main menu, select Dynamic DNS.

b. Select the **DynDNS.org** radio button to display the following screen:

c. Fill in the fields with the account and host name settings.

- In the **Host and Domain Name** field enter **fvl328.dyndns.org**.
- In the **User Name** field, enter the account user name.
- In the **Password** field, enter the account password.

d. Click **Apply.**

e. Click **Show Status**.

The resulting screen should show Update OK: good:
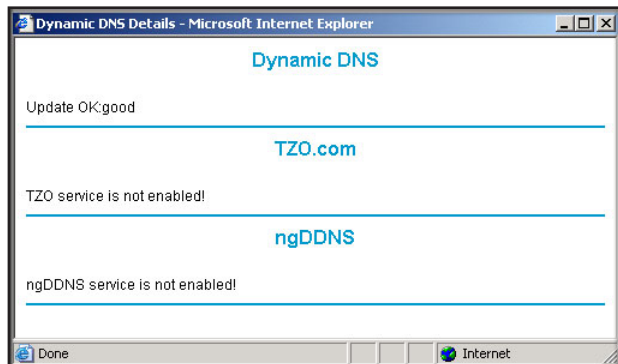
4. Configure the DGN2200v3 as in the gateway-to-gateway procedures using the VPN Wizard (see *Set Up a Gateway-to-Gateway VPN Configuration* on page 108), being certain to use appropriate network addresses for the environment.

The LAN addresses used in this example are as follows:

Device	LAN IP Address	LAN Subnet Mask
DGN2200v3	10.5.6.1	255.255.255.0
FVL328	172.23.6.1	255.255.255.0

a. Enter **toFVL328** for the connection name.

b. Enter **fvl328.dyndns.org** for the remote WAN's IP address.

c. Enter the following:
   - IP Address: **172.23.9.1**
   - Subnet Mask: **255.255.255.0**

5. Configure the FVL328 as in the gateway-to-gateway procedures for the VPN Wizard (see *Set Up a Gateway-to-Gateway VPN Configuration* on page 108), being certain to use appropriate network addresses for the environment.

a. Enter **toDG834** for the connection name.

b. Enter **dg834g.dyndns.org** for the remote WAN's IP address.

c. Enter the following:
   - IP Address: **10.5.6.1**
   - Subnet Mask: **255.255.255.0**

6. Test the VPN tunnel by pinging the remote network from a PC attached to the DGN2200v3.

a. Open the command prompt (Start -> Run -> cmd)

b. Type `ping 172.23.9.1`

```
C:\WINNT\system32\ping.exe                                    _ □ X

Pinging 172.23.9.1 with 32 bytes of data:

Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
```
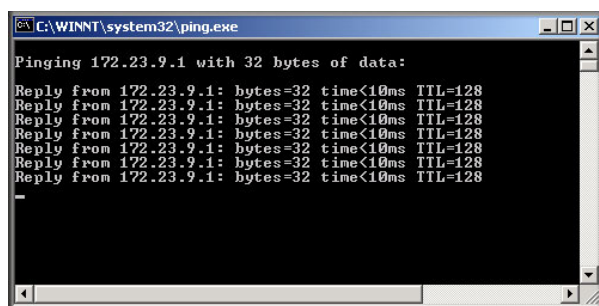
If the pings fail the first time, try the pings a second time.

Configuration Summary (Telecommuter Example)

The configuration in this section follows the addressing and configuration mechanics defined by the VPN Consortium. Gather the necessary information before you begin configuration. Verify that the firmware is up to date, and make sure you have all the addresses and parameters to be set on both sides. Assure that there are no firewall restrictions.

VPN Consortium Scenario	Scenario 1
Type of VPN:	PC/client-to-gateway, with client behind NAT router
Security scheme:	IKE with pre-shared secret/key (not certificate based)
IP addressing:	
Gateway	Fully qualified domain name (FQDN)
Client	Dynamic

192.168.0.1/24
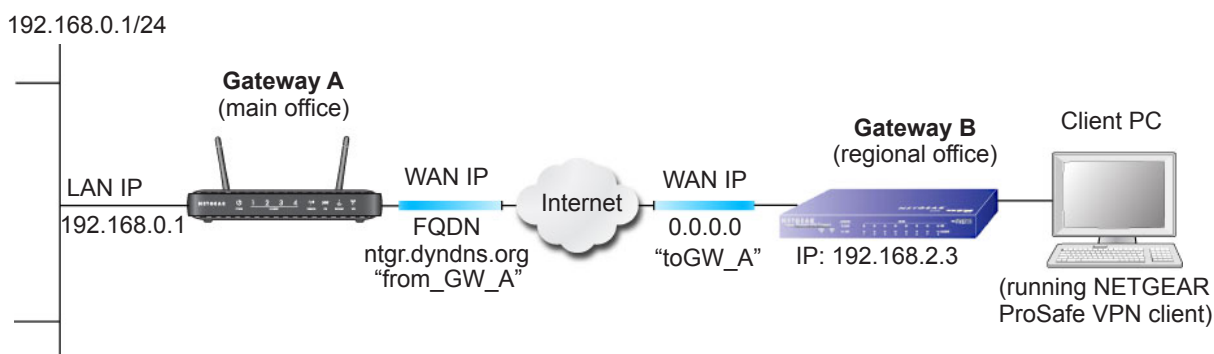
Figure 17. Telecommuter Example

Setting Up Client-to-Gateway VPN Configuration

Setting up a VPN between a remote PC running the NETGEAR ProSafe VPN Client and a network gateway involves two steps:

Step 1: Configure Gateway A (Router at the Main Office)

1. Log in to the VPN router. Select **VPN Policies** to display the VPN Policies screen. Click **Add Auto Policy**.

2. Enter the following information, based on your individual setup:

   - **Policy Name**. In this example, f*rom GW_A* is used.

   - **IKE Keep Alive**: This is optional. It has to match the value in the Remote LAN IP Address field when enabled. (The remote computer has to respond to pings.)

   - **Remote LAN**. In this example, the IP address is *192.168.2.3*. The remote NAT router has to have address reservation set and VPN Passthrough enabled.

   - **IKE Local Identity Type and Remote Identity Type**. In this example, the fully qualified domain names used are *from GW_A.com* and *toGW_A.com*.

3. Click **Apply** when you are finished to display the VPN Policies screen.

VPN Policies							
				Back	Cancel	Apply	
Policy Table							
	#	Enable	Name	Type	Local	Remote	ESP
⦿	1	☑	GtoClient	Auto	192.168.0.1 / 255.255.255.0	---	3DES
			Edit		Delete		
			Add Auto Policy		Add Manual Policy		

4. To view or modify the tunnel settings, select the radio button next to the tunnel entry, and then click **Edit**.

Step 2: Configure Gateway B (Router at the Regional Office)

This procedure assumes that the PC running the client has a dynamically assigned IP address. The PC needs to have a VPN client program installed that supports IPSec (in this case study, the NETGEAR VPN ProSafe Client is used). Go to the NETGEAR website (*www.netgear.com*) for information about how to purchase the NETGEAR ProSafe VPN Client.

> **Note:** Before installing the software, be sure to turn off any virus protection or firewall software you might be running on your PC.

1. Install the NETGEAR ProSafe VPN Client on the remote PC, and then reboot.

   a. You might need to insert your Windows CD to complete the installation.

   b. If you do not have a modem or dial-up adapter installed in your PC, you might see the warning message stating "The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed." You can disregard this message.

   c. Install the IPSec component. You might have the option to install either the VPN adapter or the IPSec component or both. The VPN adapter is not necessary.

   d. The system should show the ProSafe icon (⌧) in the system tray after rebooting.

e. Double-click the system tray icon to open the Security Policy Editor.
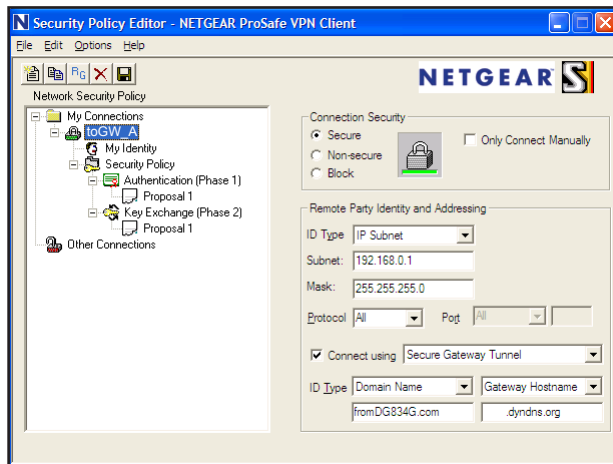
2. Add a new connection.

a. Run the NETGEAR ProSafe Security Policy Editor program, and create a VPN Connection.

b. From the Edit menu of the Security Policy Editor, select **Add > Connection**. A New Connection listing appears in the list of policies.

c. Rename the new connection to match the connection name you entered in the VPN settings of Gateway A. Choose connection names that make sense to the people using and administrating the VPN.
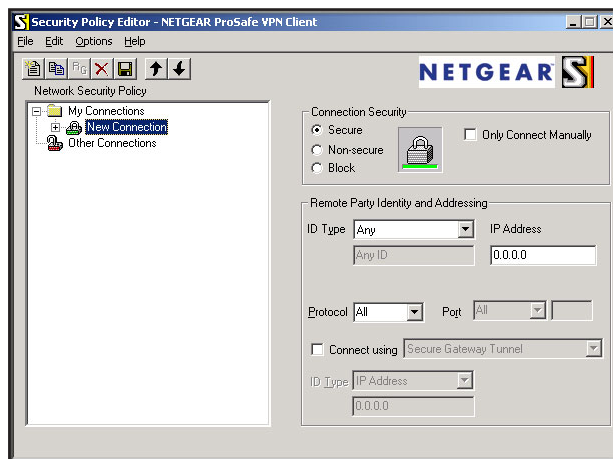
Note: *In this example, the connection name on the client side of the VPN tunnel is **toGW_A**. It does not have to match the VPN_client connection name used on the gateway side of the VPN tunnel because connection names do not affect how the VPN tunnel functions.*

d. Select **Secure** in the Connection Security section.

e. Select **IP Subnet** in the **ID Type** drop-down list.

    f.   In this example, type **192.168.0.1** in the **Subnet** field as the network address of the modem router.

    g. Enter **255.255.255.0** in the **Mask** field as the LAN subnet mask of the modem router.

    h. Select **All** in the **Protocol** drop-down list to allow all traffic through the VPN tunnel.

    i.   Select the **Connect using Secure Gateway Tunnel** check box.

    j.   Select **Domain Name** in the **ID Type** drop-down list, and enter **fromGW_A.com** (in this example).

    k. Select **Gateway Hostname** and enter **ntgr.dyndns.org** (in this example).

3. Configure the security policy in the modem router software.

    a. In the Network Security Policy list, expand the new connection by double-clicking its name or clicking the + symbol. My Identity and Security Policy appear below the connection name.

    b. Click **Security Policy** to show the Security Policy screen.
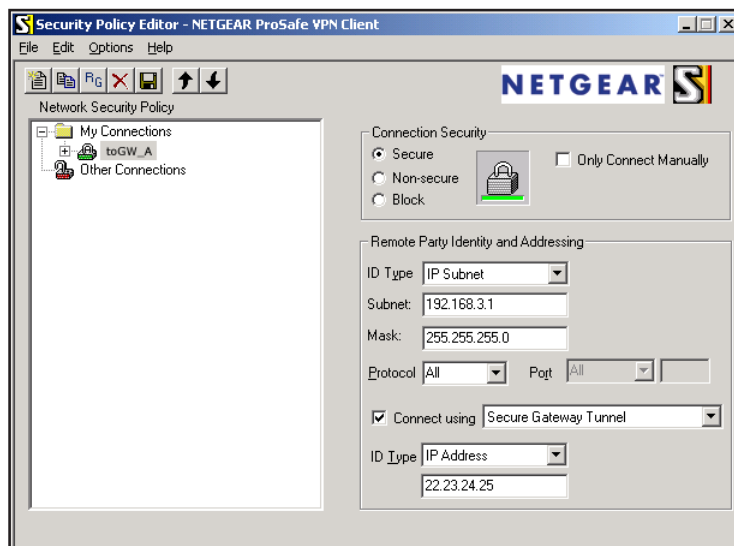
    c. Select the **Main Mode** radio button in the Select Phase 1 Negotiation Mode group.

4. Configure the VPN client identity.

In this step, you provide information about the remote VPN client PC. You have to provide the pre-shared key that you configured in the modem router and either a fixed IP address or a fixed virtual IP address of the VPN client PC.

a. In the Network Security Policy list on the left side of the Security Policy Editor window, click **My Identity**.
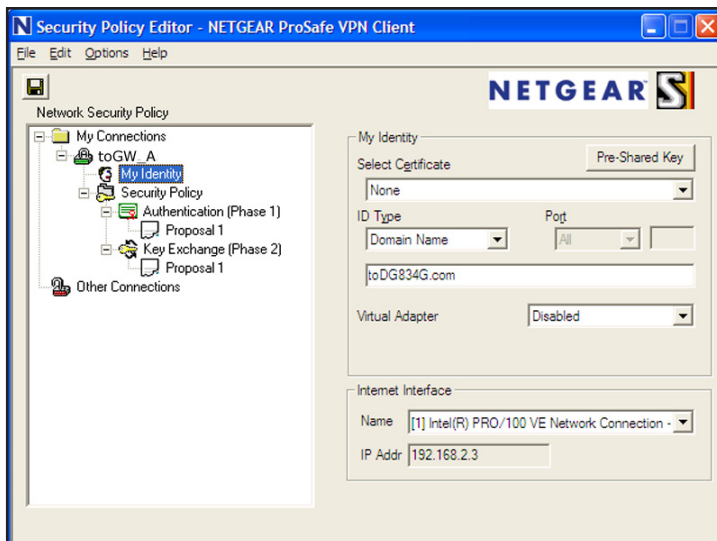
b. Select **None** in the **Select Certificate** field.

c. Select **Domain Name** in the **ID Type** field, and enter **toGW_A.com** (in this example). Select **Disabled** in the **Virtual Adapter** field.

d. In the Internet Interface section, select **Intel PRO/100VE Network Connection** (in this example; your Ethernet adapter might be different) in the **Name** field, and then enter **192.168.2.3** (in this example) in the **IP Addr** field.

e. Click the **Pre-Shared Key** button.

f. In the Pre-Shared Key screen, click **Enter Key**. Enter the DGN2200v3's pre-shared key and click **OK**. In this example, **12345678** is entered, though the screen shows asterisks. This field is case-sensitive.

5. Configure the **VPN Client Authentication Proposal**.

In this step, you provide the type of encryption (DES or 3DES) to be used for this connection. This selection has to match your selection in the VPN router configuration.

a. In the Network Security Policy list on the left side of the Security Policy Editor window, expand the Security Policy heading by double-clicking its name or clicking the + symbol.

b. Expand the Authentication subheading by double-clicking its name or clicking the + symbol. Then select Proposal 1 below Authentication.
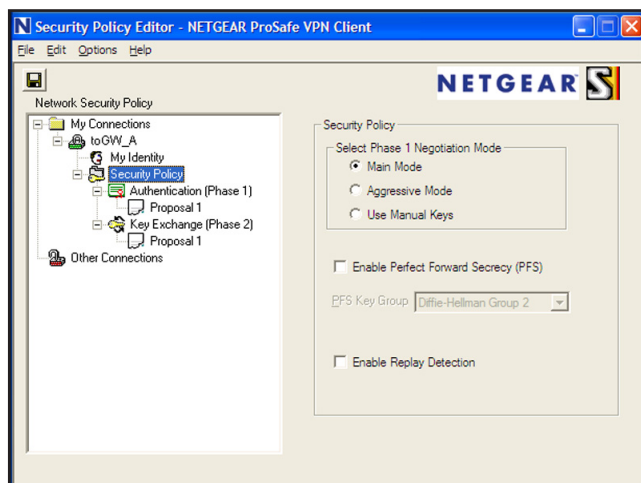
c. In the **Authentication Method** drop-down list, select **Pre-Shared Key**.

d. In the **Encrypt Alg** drop-down list, select the type of encryption. In this example, use **Triple DES**.

e. In the **Hash Alg** drop-down list, select **SHA-1**.

f. In the **SA Life** drop-down list, select **Unspecified**.

g. In the **Key Group** drop-down list, select **Diffie-Hellman Group 2**.

6. Configure the **VPN Client Key Exchange Proposal**.

In this step, you provide the type of encryption (**DES** or **3DES**) to be used for this connection. This selection has to match your selection in the VPN router configuration.

a. Expand the Key Exchange subheading by double-clicking its name or clicking the + symbol. Then select Proposal 1 below Key Exchange.
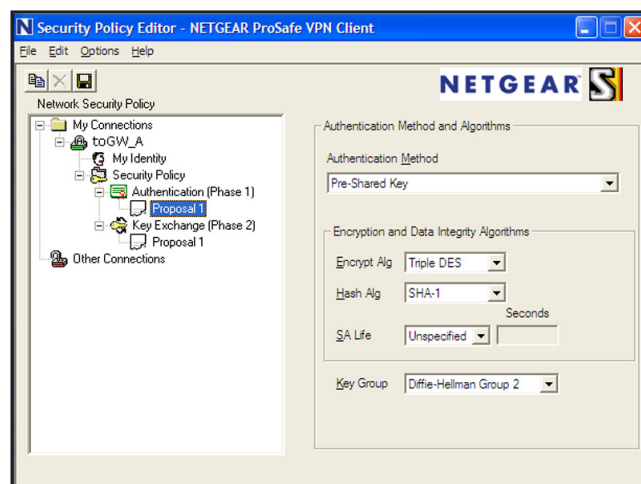
b. In the **SA Life** drop-down list, select **Unspecified**.

c. In the **Compression** drop-down list, select **None**.

d. Select the **Encapsulation Protocol (ESP)** check box.

e. In the **Encrypt Alg** drop-down list, select the type of encryption. In this example, use **Triple DES**.

f. In the **Hash Alg** drop-down list, select **SHA-1**.

g. In the **Encapsulation** drop-down list, select **Tunnel**.

h. Leave the **Authentication Protocol (AH)** check box cleared.

7. Save the VPN Client settings.

From the File menu at the top of the Security Policy Editor window, select **Save**.

After you have configured and saved the VPN client information, your PC automatically opens the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router's LAN.

8. Check the VPN connection.

To check the VPN connection, you can initiate a request from the remote PC to the VPN router's network by using the Connect option in the modem router screen:
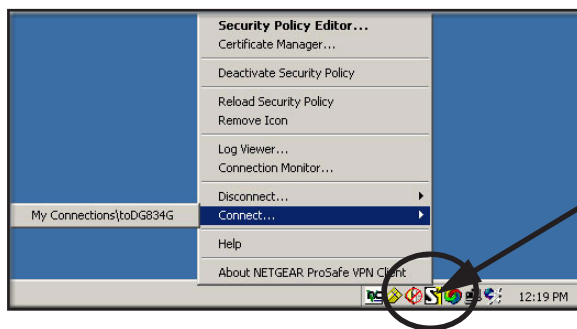
Right-click the system tray icon to open the pop-up menu.

Since the remote PC has a dynamically assigned WAN IP address, it has to initiate the request.

a. Right-click the system tray icon to open the pop-up menu.

b. Select Connect to open the My Connections list.

c. Select toDGN2200.

The modem router reports the results of the attempt to connect. Once the connection is established, you can access resources of the network connected to the VPN router.

Right-click the system tray icon to open the pop-up menu.

To perform a ping test using this example, start from the remote PC:

a. Establish an Internet connection from the PC.

b. On the Windows taskbar, click the **Start** button, and then select **Run**.

c. Type `ping -t 192.168.0.1`, and then click **OK**.
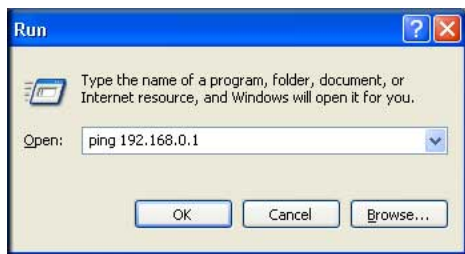
This causes a continuous ping to be sent to the VPN router. Within 2 minutes, the ping response should change from `timed out` to `reply`.

Once the connection is established, you can open the browser on the PC and enter the LAN IP address of the VPN router. After a short wait, you should see the login screen of the VPN router (unless another PC already has the VPN router management interface open).

> **Note:** You can use the VPN router diagnostics to test the VPN connection from the VPN router to the client PC. To do this, select Diagnostics on the modem router main menu.

Monitoring the VPN Tunnel

To view information about the progress and status of the VPN client connection, open the Log Viewer. In Windows, click **Start**, and select **Programs > N300 Wireless ADSL2+ Modem Router DGN2200v3 > Log Viewer**.

> **Note:** Use the active VPN tunnel information and pings to determine whether a failed connection is due to the VPN tunnel or some reason outside the VPN tunnel.

The Connection Monitor screen displays:
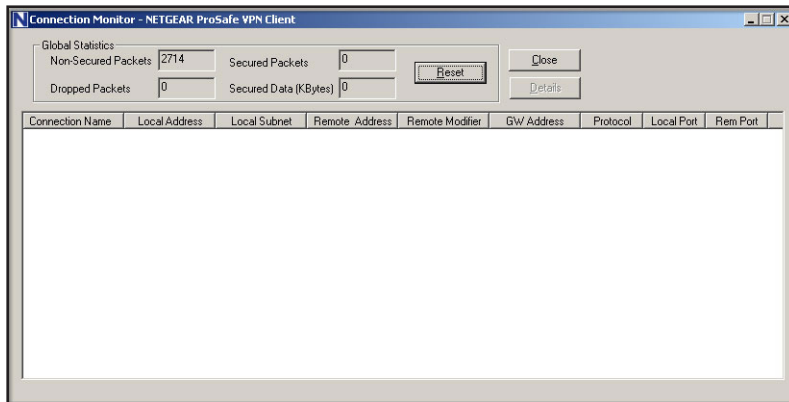
While the connection is being established, the connection name listed in this screen shows SA before the name of the connection. When the connection is successful, the SA changes to the yellow key symbol.

Note: While your PC is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you need to close the VPN connection to have normal Internet access.

Viewing the VPN Router's VPN Status and Log Information

To view information about the status of the VPN client connection, open the VPN router's VPN Status screen:

1. Select **VPN Status**. The VPN Status/Log screen displays:
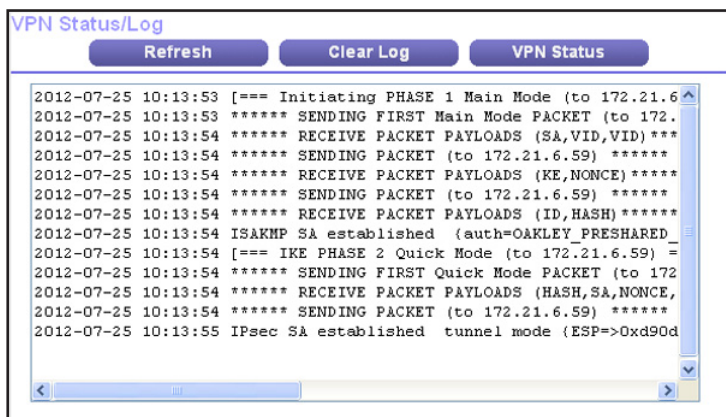
2. To view the VPN tunnels status, click **VPN Status**.

Current VPN Tunnels (SAs)

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	d90dc994	d924fef5	111	172.21.6.59	Drop	3549	3600

Notification of Compliance

NETGEAR Wireless Routers, Gateways, APs

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

Products bearing the C E marking comply with the following EU directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

If this product has telecommunications functionality, it also complies with the requirements of the following EU Directive:

- R&TTE Directive 1999/5/EC

Compliance with these directives implies conformity to harmonized European standards that are noted in the EU Declaration of Conformity.

Intended for indoor use only in all EU member states, EFTA states, and Switzerland.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the N300 Wireless ADSL2+ Modem Router DGN2200v3 complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA / Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
- Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.
- Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (N300 Wireless ADSL2+ Modem Router DGN2200v3) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Caution:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Interference Reduction Table

The table below shows the Recommended Minimum Distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters

Index